XpoLog Center V3.0
User Manual

XpoLog Home page

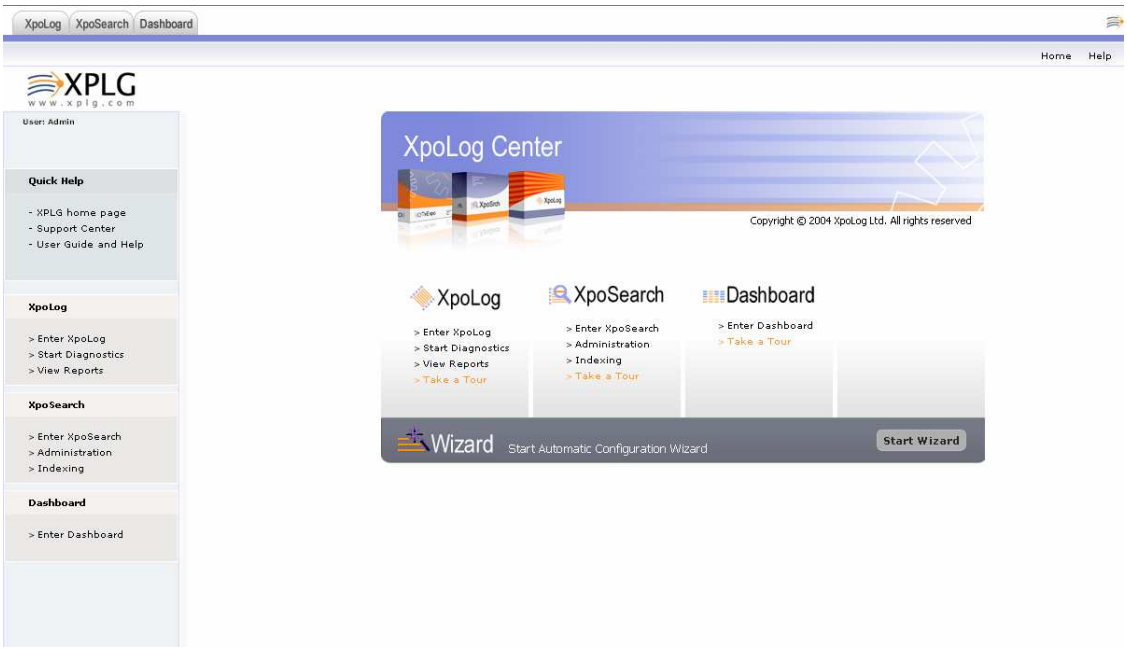
This is the XpoLog's main page. In case security is activated, you will be automatically redirected to a login page.

In the main XpoLog Home page you will find 3 main tabs:

1) XpoLog
2) XpoSearch
3) Dashboard

On the left pane there are a few quick links to XpoLog's help and to the main features as well: XpoLog, XpoSearch and Dashboard.

In the upper right corner there are two links: Home and Help. The Home link will lead back to XpoLog's home page, and Help will open XpoLog's help guide.



XpoLog

Left Pane

When a log is selected and displayed in the main log view, the left pane is extended to include the following options:

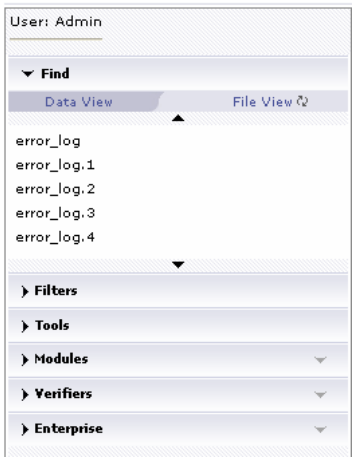
Find

The Find section has two tabs in it: Data view and File view.

The data view acts the same as the quick filter from the log view, with the addition of available time filters that can be set in advance.

The file view displays a list of all the files that are part of the specific log. You can refresh the list by clicking the icon. You may browse through the list using the up and down arrows.

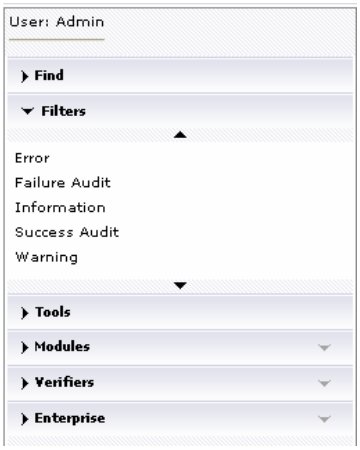
Find – Data View



Find – File view

Filters

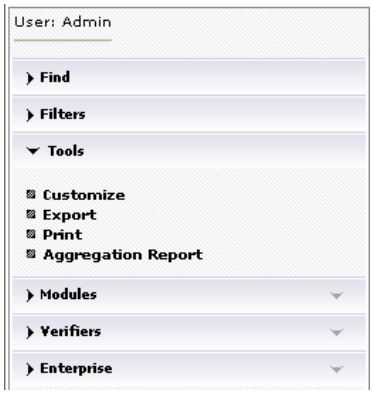
The list of predefined filters is displayed (not quick filters). You may browse through the list using the up and down arrows.



List of available filters

Tools

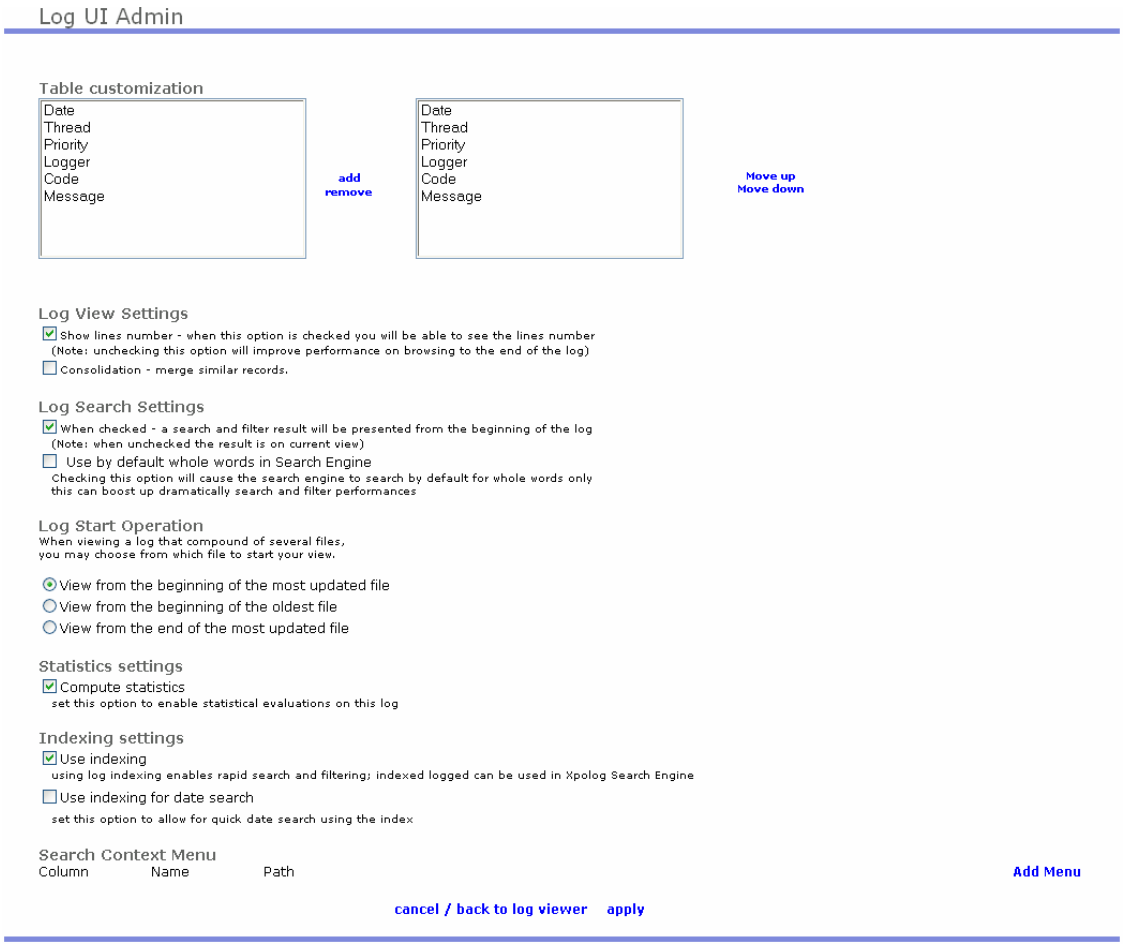
Inside the tools tab you will find four options: Customize, Export, Print and Aggregation report.



The list of Tools options

- Customize – via this screen you can customize the logs view properties.
    - Table customization: Add/Remove or move Up/Down any column from the available columns list.
    - Priority color selection: If you want events of different priorities to be displayed in different colors, select the 'Use priority colors' options; select for each of the priorities in the list a color by clicking on the 'Pick color' link and choosing the desired color.
    - Log view settings:
        - Show lines number – check this option in case you would like XpoLog to display line number in the log view.
        - Consolidation – check this option to merge records whose whole data other than the date is identical into one record.
    - Log search settings:
        - Check this option in case you would like XpoLog to present a search and filter result from the beginning of the log
        - Use by default whole words in Search Engine - Checking this option will cause the search engine to search by default for whole words only. Using this option will expedite the searches and filters processes.
    - Log start operation - In case a log is composed of more than one file, you may select the file display order as following:
        - View from the beginning of the most updated file
        - View from the beginning of the oldest file
        - View from the end of the most updated file

- Statistics settings – Check this option in order to allow statistical computations for this log. For more information, go to Dashboard.
- Indexing setting – Check this option to allow faster searches and filtering. For more information, go to XpoSearch → Indexing.
- Indexing for date search - Check this option to allow fast date searches.
- Search context menu - Add a search context menu to a log by specifying the relevant columns, the name of the data repository (i.e. Google) and the URL to be used for the search.

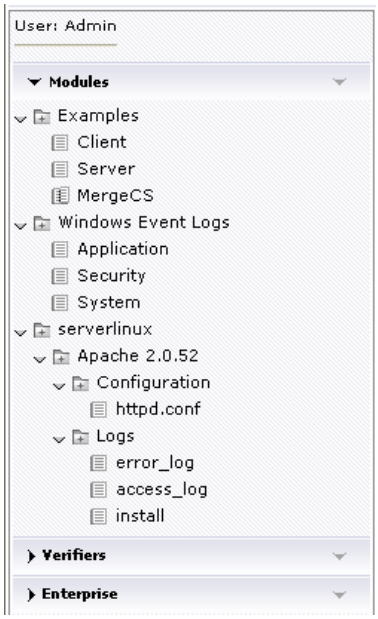


The customize log screen

- Export – Exporting the log using various export methods. For further information, please read about Data support → Export log.
- Print – Clicking this link will open the log in a separate window ready to print.
- Aggregation Report – This wizard helps you to create a quick aggregation report on the specific log. For further information, please read the Reports chapter.

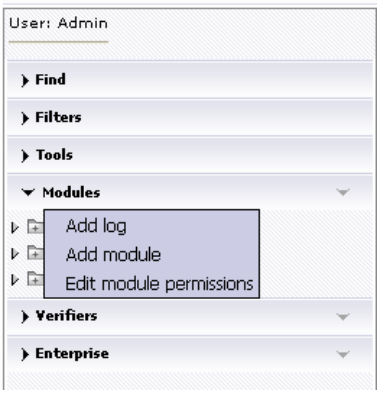
Modules

Under the modules you will find XpoLog's main tree.

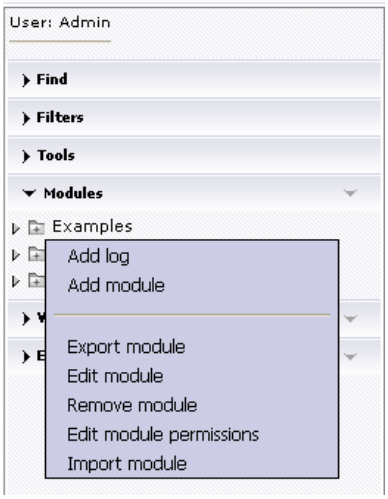


XpoLog tree, located under Modules

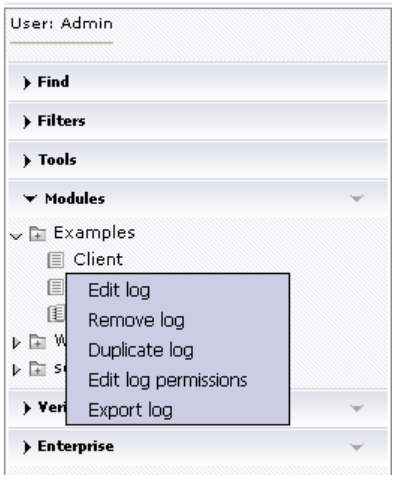
- Click the modules' arrow ( ) in order to add a log, add a module or edit module permissions.
    - Add log – Add a new log to XpoLog. For further information, please go to Administration → add log
    - Add module – Add a new module to XpoLog. For further information, please go to Administration → add module.
    - Edit module permissions – Edit permission is available only when security is activated. For further information, please go to Security.



- Right click one of the modules. A menu is opened with the following options:
    - Add log – Add a new log to XpoLog. For further information, please go to Administration → add log
    - Add module – Add a new module to XpoLog. For further information, please go to Administration → add module
    - Export module – allows you to export the module with all its data. For further information, please go to Data Support → Export module
    - Edit module – allows you to edit data such as name/owner/parent module and module's members. For further information, please go to Administration → Edit module
    - Remove module – Allows you to remove a module. For further information, please go to Administration → Remove module
    - Import module – Allows you to import a module to XpoLog. For further information, please go to Data support → Import module

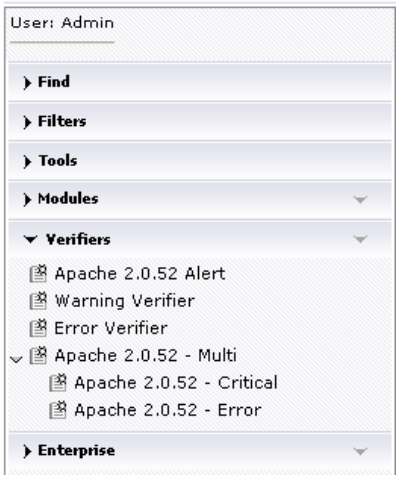


- Right click one of the logs. A menu is opened with the following options:
    - Edit log – Edit an existing log. For further information, please go to Administration → Edit log
    - Remove log – Allows you to remove a log from the system. For further information, please go to Administration → Remove log
    - Duplicate log – Allows you to duplicate the log by going through the log's wizard
    - Export Log – Allows you to export the log using various methods.
      For further information, please read about Data support → Export log.



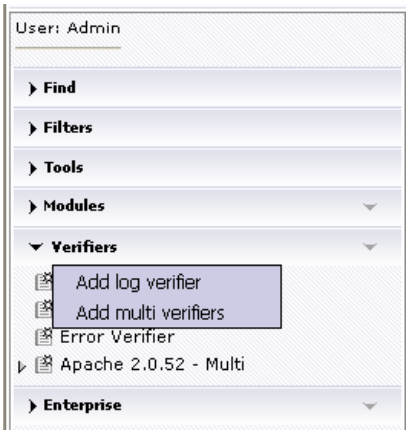
Verifiers

The list of all predefined log verifiers is displayed.

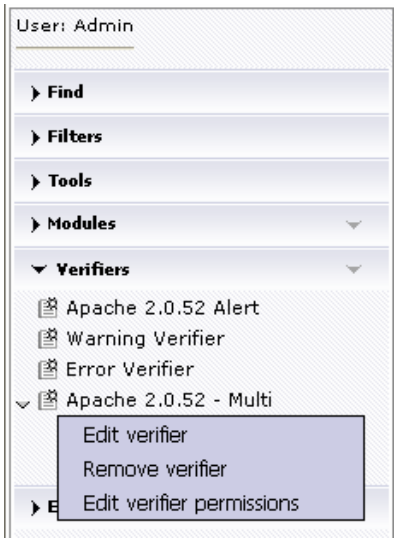


The list of verifiers and multi verifiers in XpoLog

- Click the verifiers' arrow ( ) in order to add a log verifier or add a multi log verifier.
    - Add a log verifier – Add a new log verifier to XpoLog. For further information, please go to Administration → Add verifier
    - Add a multi log verifier – Add a multi log verifier to XpoLog. For further information, please go to Administration → Add verifier

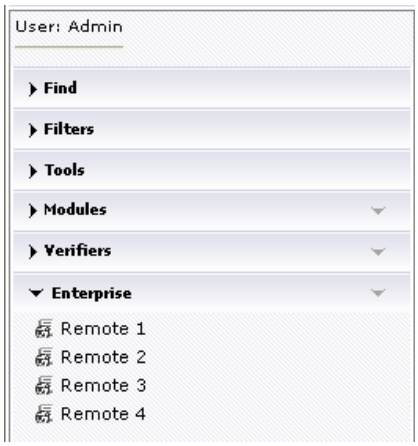


- Right click one of the verifiers. A menu is opened with the following options:
  - Edit verifier – Edit an existing verifier. For further information, please go to Administration → Edit verifier
  - Remove verifier – Allows the user to remove the verifier from the system. For further information, please go to Administration → Remove verifier
  - Edit verifier's permission - Edit permission is available only when security is activated. For further information, please go to Security



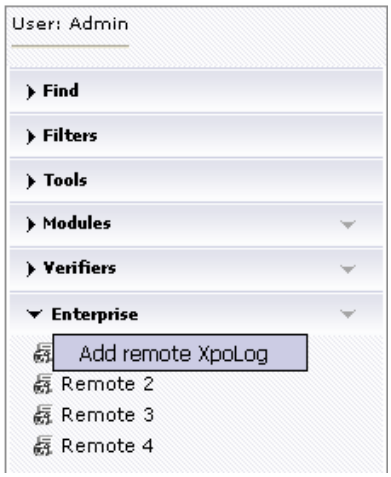
Enterprise

the list of all the remote XpoLogs is displayed.

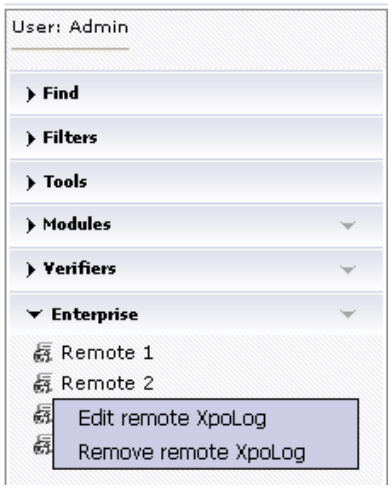


The list of remote XpoLog nodes

- Click the Enterprise's arrow ( ) in order to add a remote XpoLog
    - Add remote XpoLog – allows you to add a remote XpoLog. For further information, please go to Data Support → Enterprise.



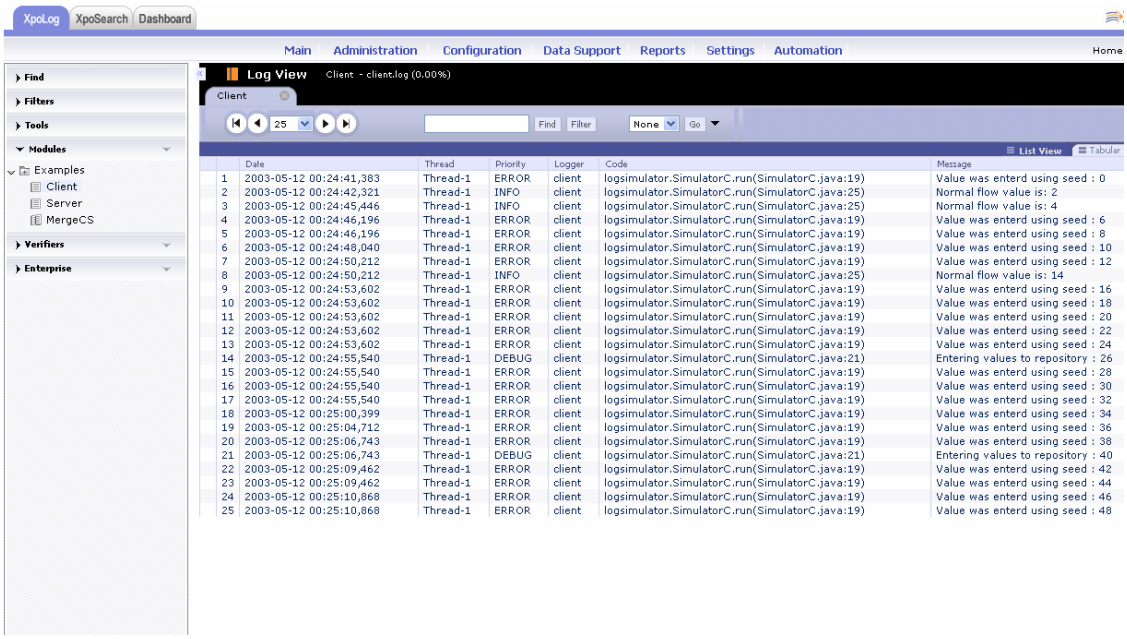
- Right click one of the remote XpoLogs. A menu is opened with the following options:
    - Edit remote XpoLog – Allows you to edit the remote XpoLog details. For further information, please go to Data Support → Enterprise.
    - Remove remote XpoLog - Allows you to remove a remote XpoLog. For further information, please go to Data Support → Enterprise.


User: Admin
Find
Filters
Tools
Modules
Verifiers
Enterprise
Remote 1
Remote 2
Edit remote XpoLog
Remove remote XpoLog

Main menu

Log View

Main screen



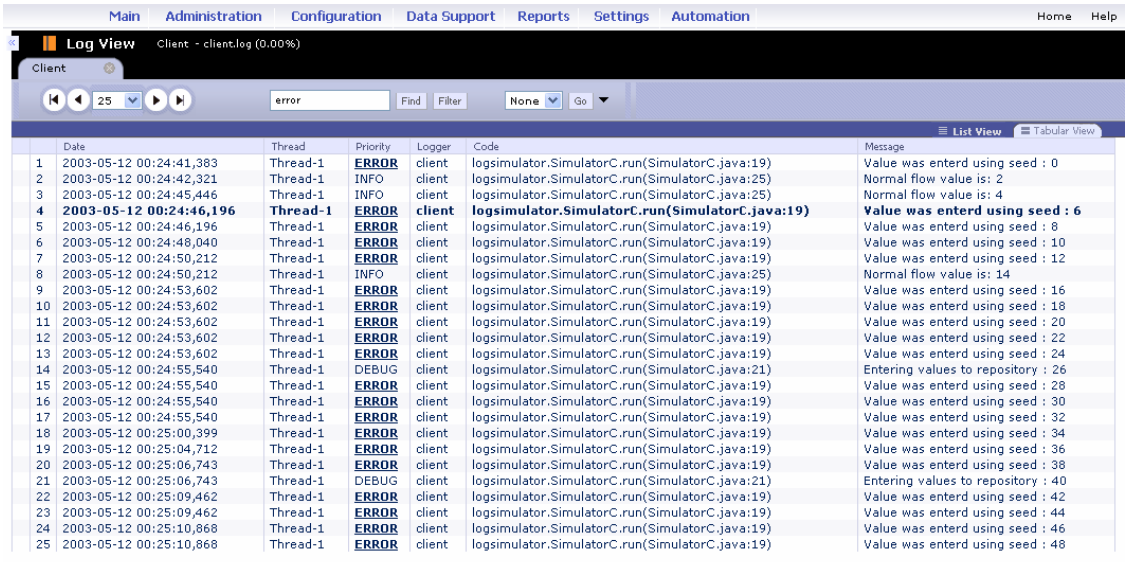
In order to start viewing a log, click one of the available logs in XpoLog's tree, located in the left pane under Modules.

Once a log is selected, it is presented in the log view screen.

In the main log view, each log is opened in a separate tab.

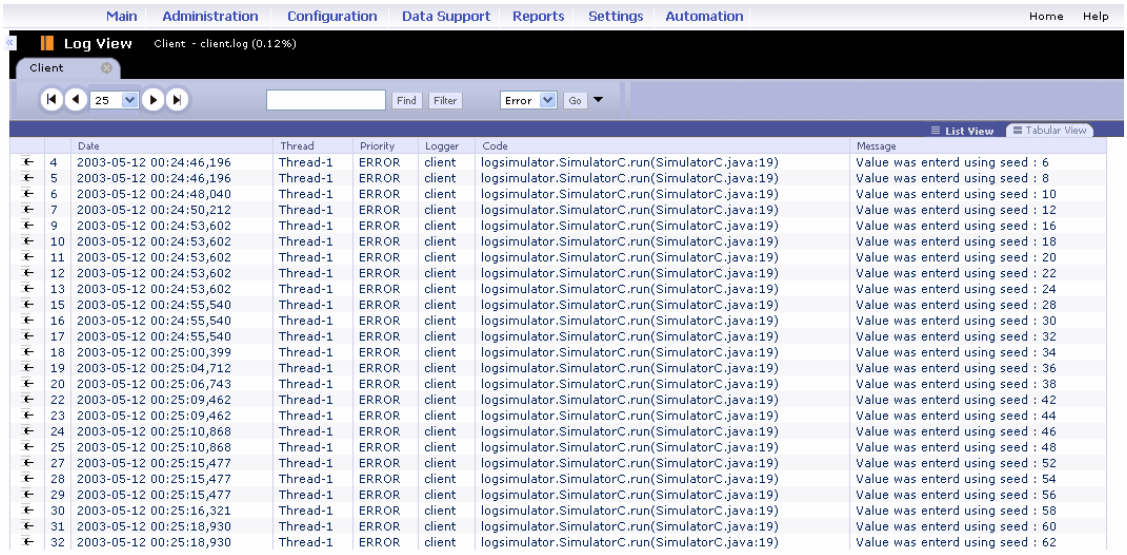
In the log's tab, one will find the following options:

- Navigation  . The left arrow will direct the user to the beginning of the log. The next two arrows will display the next records available, according to the 'number of records to display' selected in the menu in between those arrows. There are five different display options: 25, 50, 100, 250, and 500 records to display. The last arrow on the right will direct the user to the end of the log.
- Quick find/filter  . In order to search a specific string in the log, enter it to the quick find field and click 'Find'. For example, try searching the phrase: "Error" via the quick filter. The results are highlighted in the log where available:



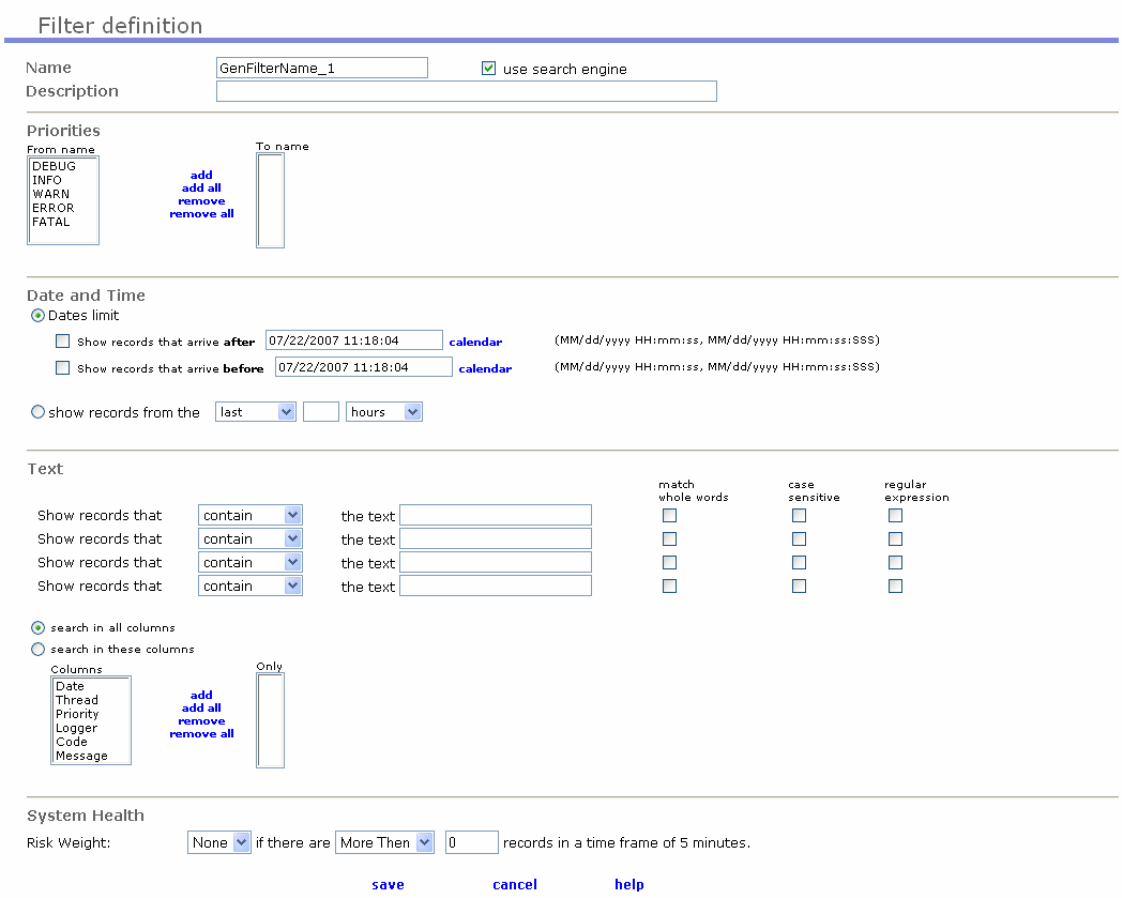
	Date	Thread	Priority	Logger	Code	Message
1	2003-05-12 00:24:41,383	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 0
2	2003-05-12 00:24:42,321	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 2
3	2003-05-12 00:24:45,446	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 4
4	**2003-05-12 00:24:46,196**	**Thread-1**	**ERROR**	**client**	**logsimulator.SimulatorC.run(SimulatorC.java:19)**	**Value was enterd using seed : 6**
5	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 8
6	2003-05-12 00:24:48,040	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 10
7	2003-05-12 00:24:50,212	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 12
8	2003-05-12 00:24:50,212	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 14
9	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 16
10	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 18
11	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 20
12	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 22
13	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 24
14	2003-05-12 00:24:55,540	Thread-1	DEBUG	client	logsimulator.SimulatorC.run(SimulatorC.java:21)	Entering values to repository : 26
15	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 28
16	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 30
17	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 32
18	2003-05-12 00:25:00,399	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 34
19	2003-05-12 00:25:04,712	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 36
20	2003-05-12 00:25:06,743	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 38
21	2003-05-12 00:25:06,743	Thread-1	DEBUG	client	logsimulator.SimulatorC.run(SimulatorC.java:21)	Entering values to repository : 40
22	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 42
23	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 44
24	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 46
25	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 48

In case you want to see only the relevant searched results, the filter command should be used. Enter the same phrase to the quick filter field, and click filter. The results should be displayed in the following way:



		Date	Thread	Priority	Logger	Code	Message
←	4	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 6
←	5	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 8
←	6	2003-05-12 00:24:48,040	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 10
←	7	2003-05-12 00:24:50,212	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 12
←	9	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 16
←	10	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 18
←	11	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 20
←	12	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 22
←	13	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 24
←	15	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 28
←	16	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 30
←	17	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 32
←	18	2003-05-12 00:25:00,399	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 34
←	19	2003-05-12 00:25:04,712	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 36
←	20	2003-05-12 00:25:06,743	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 38
←	22	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 42
←	23	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 44
←	24	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 46
←	25	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 48
←	27	2003-05-12 00:25:15,477	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 52
←	28	2003-05-12 00:25:15,477	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 54
←	29	2003-05-12 00:25:15,477	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 56
←	30	2003-05-12 00:25:16,321	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 58
←	31	2003-05-12 00:25:18,930	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 60
←	32	2003-05-12 00:25:18,930	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 62

- Predefined filters. Click the small arrow in order to open the filter's menu. Click 'New' the following screen is displayed:



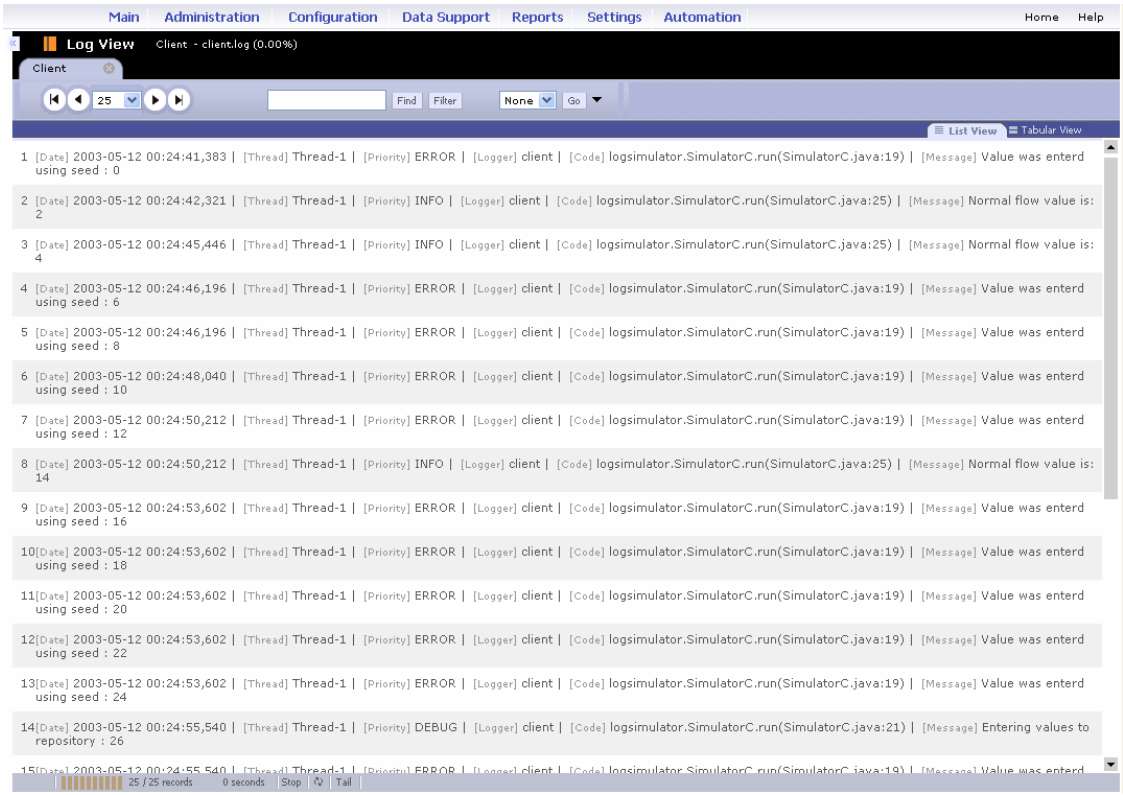
In the first section, you should provide a name to the filter and a description (Not mandatory).

In the second part of the wizard, you can select a predefined priority according to the log's pattern.

You may narrow down the filter to a specific time frame using the date and time rules.

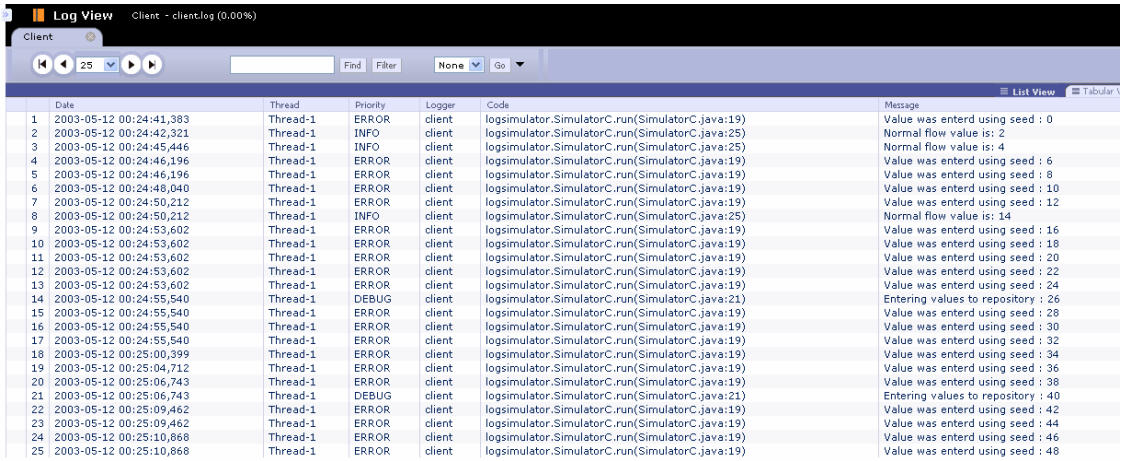
In the fourth part (Text), you may add any desired string to be filtered. You may add a filter that Contains/Not Contains/Equals/Not Equals a relevant string. Moreover, you can decide if the filtered string should be searched in all columns or from specific column/columns, by adding the relevant column to the 'only' list. When the filter definition is complete, click save. XpoLog will lead you back to the main log view screen, displaying only the filtered results.

- List View/Tabular view. You may switch between both views for your own comfort. The default view is the Tabular view. The list view will look like this:



- At the bottom of the log viewer screen you will find a progress bar, the number of records found, the time it took XpoLog to find and display the records, Stop, Refresh and Tail links. 

  The tail command is used to update the log's data in real time. It will look for new records to display every X seconds and will display them as soon as they reach a certain minimum number of records. For more info, please see: Log view settings.
- In order to open the log view in a full screen mode, click the arrows link, located in the upper left side of the log view -  . In order to return to the normal view, click the  link again:

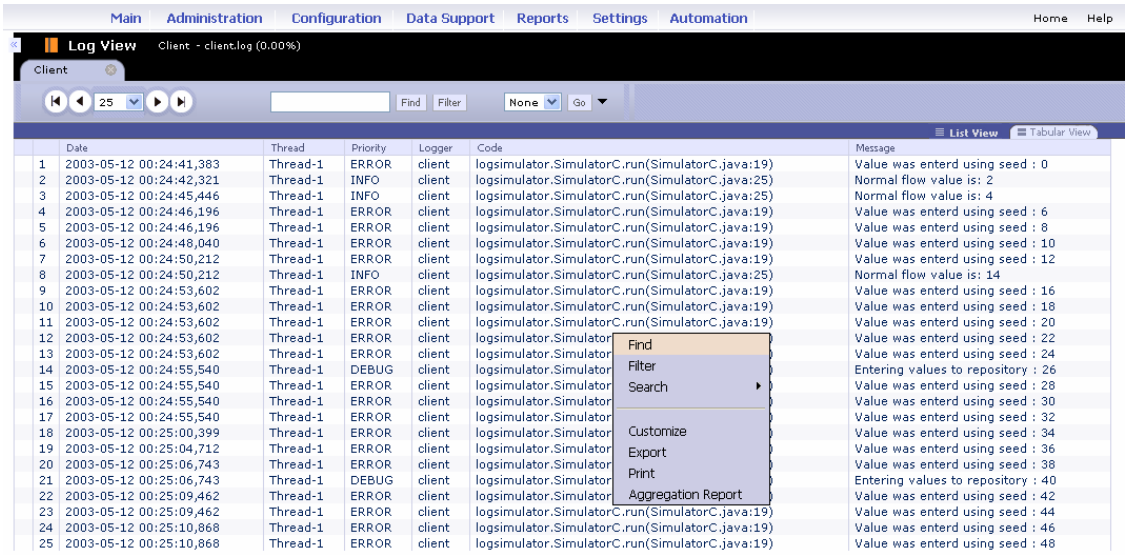


	Date	Thread	Priority	Logger	Code	Message
1	2003-05-12 00:24:41,383	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 0
2	2003-05-12 00:24:42,321	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 2
3	2003-05-12 00:24:45,446	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 4
4	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 6
5	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 8
6	2003-05-12 00:24:48,040	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 10
7	2003-05-12 00:24:50,212	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 12
8	2003-05-12 00:24:50,212	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 14
9	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 16
10	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 18
11	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 20
12	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 22
13	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 24
14	2003-05-12 00:24:55,540	Thread-1	DEBUG	client	logsimulator.SimulatorC.run(SimulatorC.java:21)	Entering values to repository : 26
15	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 28
16	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 30
17	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 32
18	2003-05-12 00:25:00,399	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 34
19	2003-05-12 00:25:04,712	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 36
20	2003-05-12 00:25:06,743	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 38
21	2003-05-12 00:25:06,743	Thread-1	DEBUG	client	logsimulator.SimulatorC.run(SimulatorC.java:21)	Entering values to repository : 40
22	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 42
23	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 44
24	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 46
25	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 48

- Right clicking the main log view will open a menu with the following options:
    - Find/Filter – Same as the quick find/filter described above.
    - Search → XpoSearch/Google.

      The specific string that was right clicked (from the log) can be searched in one of the following methods:

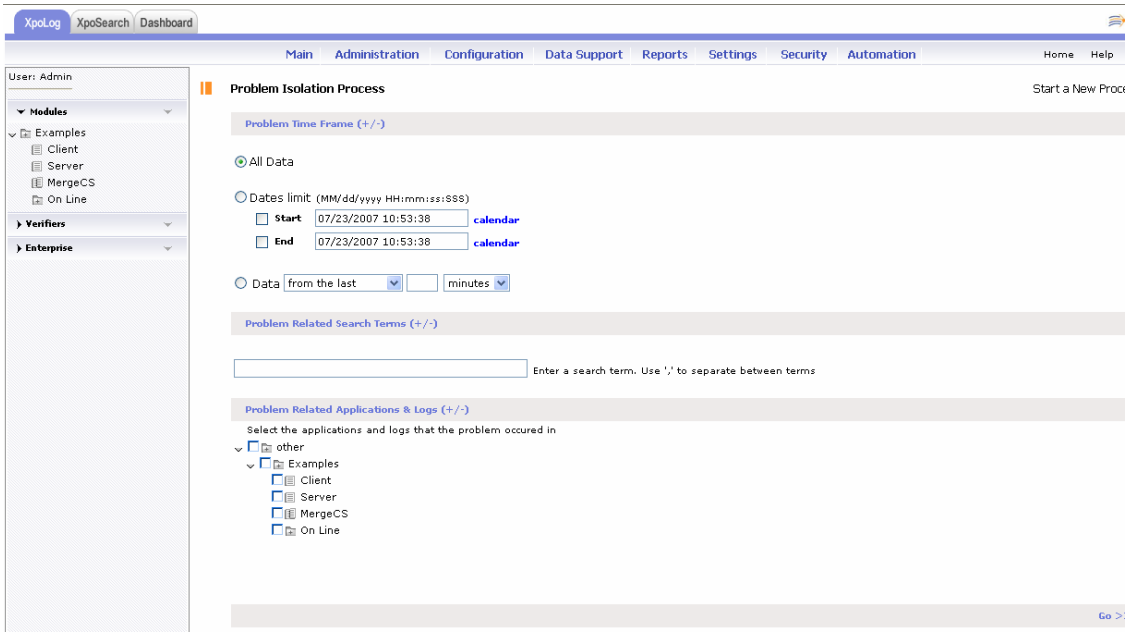
      1) XpoSearch: For further details, read the XpoSearch chapter
      2) Google: A new window is opened with the relevant string search results in Google.



	Date	Thread	Priority	Logger	Code	Message
1	2003-05-12 00:24:41,383	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 0
2	2003-05-12 00:24:42,321	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 2
3	2003-05-12 00:24:45,446	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 4
4	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 6
5	2003-05-12 00:24:46,196	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 8
6	2003-05-12 00:24:48,040	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 10
7	2003-05-12 00:24:50,212	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 12
8	2003-05-12 00:24:50,212	Thread-1	INFO	client	logsimulator.SimulatorC.run(SimulatorC.java:25)	Normal flow value is: 14
9	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 16
10	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 18
11	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 20
12	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.Simulator	Value was enterd using seed : 22
13	2003-05-12 00:24:53,602	Thread-1	ERROR	client	logsimulator.Simulator	Value was enterd using seed : 24
14	2003-05-12 00:24:55,540	Thread-1	DEBUG	client	logsimulator.Simulator	Entering values to repository : 26
15	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.Simulator	Value was enterd using seed : 28
16	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.Simulator	Value was enterd using seed : 30
17	2003-05-12 00:24:55,540	Thread-1	ERROR	client	logsimulator.Simulator	Value was enterd using seed : 32
18	2003-05-12 00:25:00,399	Thread-1	ERROR	client	logsimulator.Simulator	Value was enterd using seed : 34
19	2003-05-12 00:25:04,712	Thread-1	ERROR	client	logsimulator.Simulator	Value was enterd using seed : 36
20	2003-05-12 00:25:06,743	Thread-1	ERROR	client	logsimulator.Simulator	Value was enterd using seed : 38
21	2003-05-12 00:25:06,743	Thread-1	DEBUG	client	logsimulator.Simulator	Entering values to repository : 40
22	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.Simulator	Value was enterd using seed : 42
23	2003-05-12 00:25:09,462	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 44
24	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 46
25	2003-05-12 00:25:10,868	Thread-1	ERROR	client	logsimulator.SimulatorC.run(SimulatorC.java:19)	Value was enterd using seed : 48

    - Customize/Export/Print/Aggregation Report. For more details, please read about tools in the left pane.

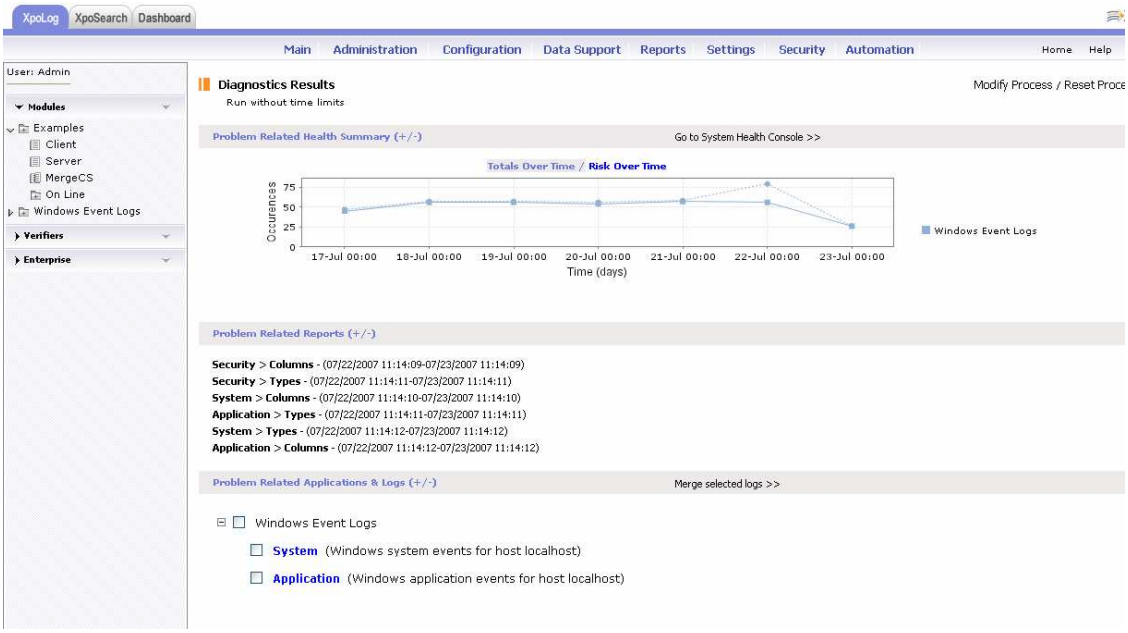
Problem Diagnostics



The problem diagnostics is where the problem isolation process starts.

Configure the relevant time frame, terms, and select the relevant logs.

When done, click ‘Go’.



The result of this process provides the following data:

- Health summary: The health summary graph provides both the total events occurred during a specific time frame and the risk level, during that time.
  For more comprehensive analysis, in the Dashboard, click the ‘Go to system health console’. For further information, please refer to the Dashboard chapter.

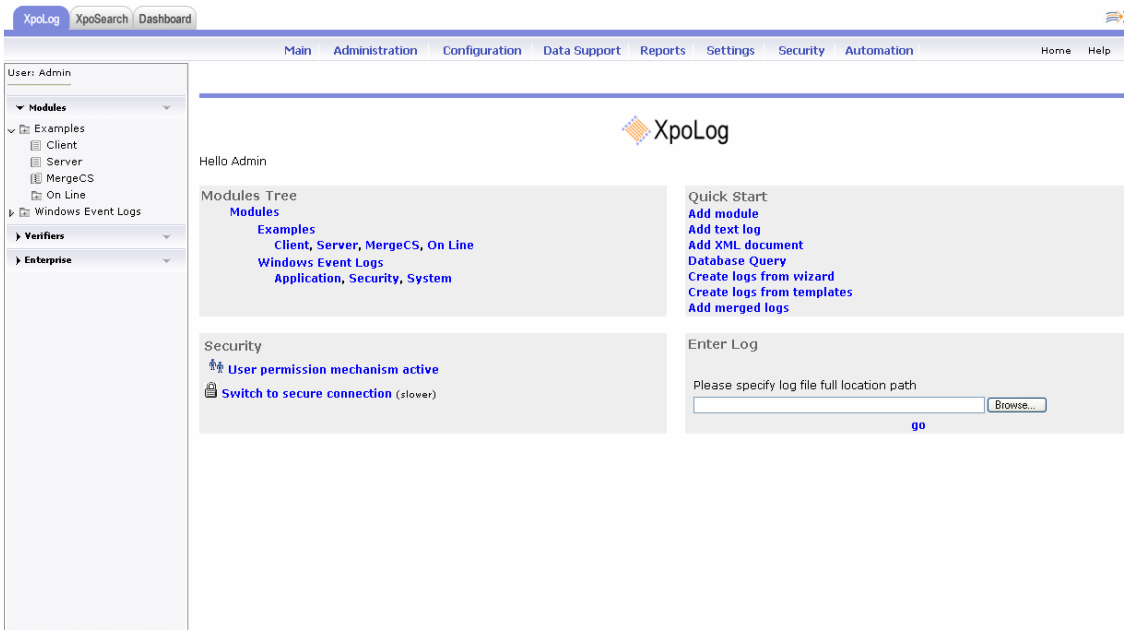
- Related reports: A list of relevant available reports in XpoLog is presented. Each report can be accessed by clicking its name. For further information, please refer to the Reports chapter.
- Related Applications and logs: A list of relevant available logs in XpoLog is presented. Each log can be accessed by clicking its name. In case there is more then one log related, XpoLog can merge them into one log and present them in the log viewer. In order to do so, select the desired logs, and click ‘Merge selected logs’.

In the upper right corner of the screen you will find two links: Modify process and Reset process.

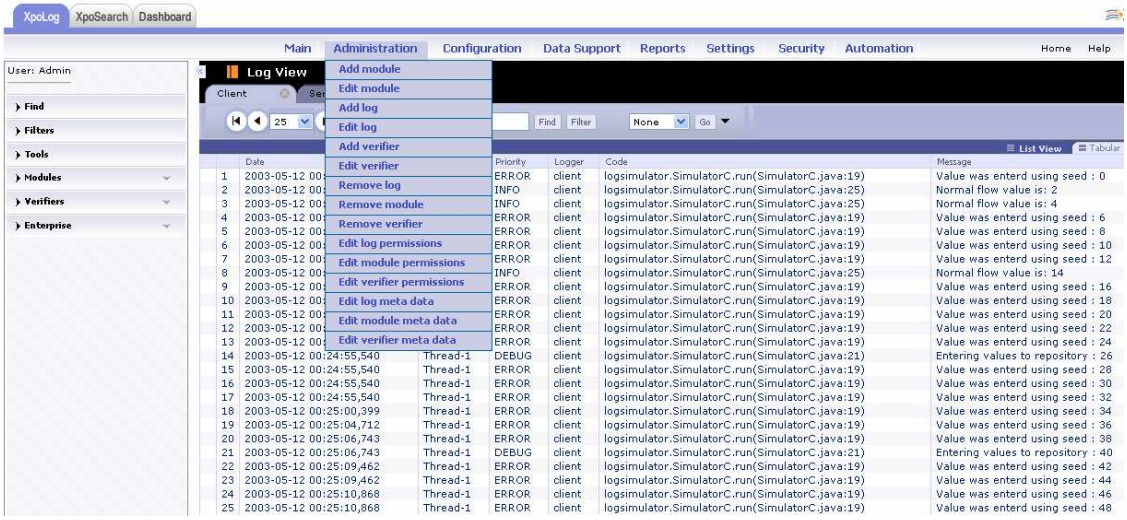
Use the first one in order to reconfigure the problem isolation process, or use the ‘Reset process’ in case you would like to start a new problem isolation process.

Portal

This is XpoLog's portal. It is about to change soon.



Administration Menu



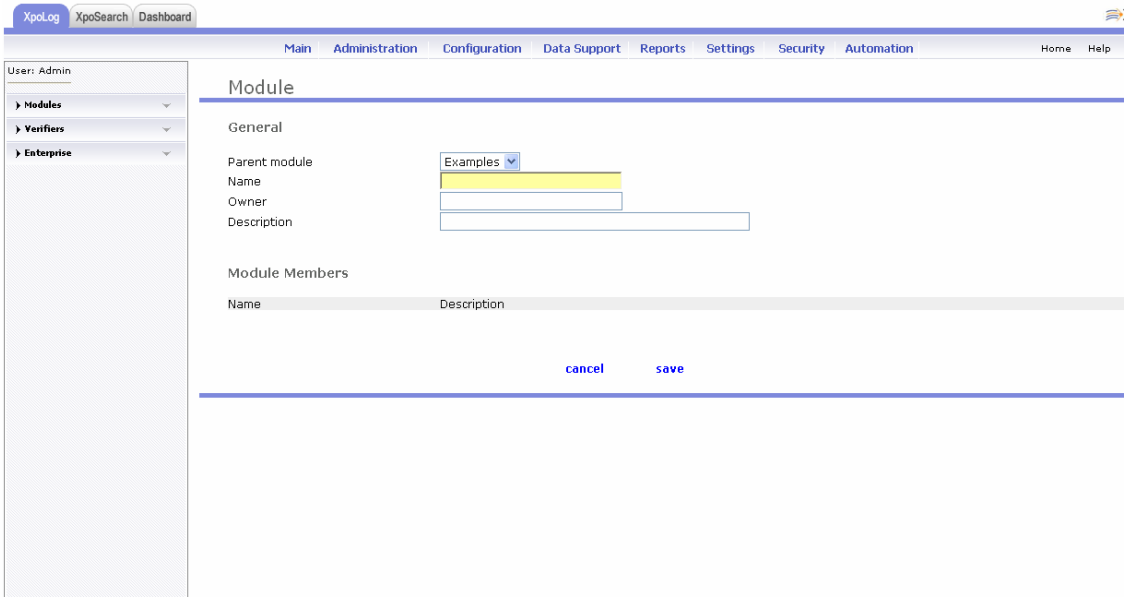
The administration menu can be divided into 3 main substances:

1) Module – Add/Edit/Remove/Permission[1]/Meta data
2) Log - Add/Edit/Remove/Permission/Meta data
3) Verifier - Add/Edit/Remove/Permission/Meta data

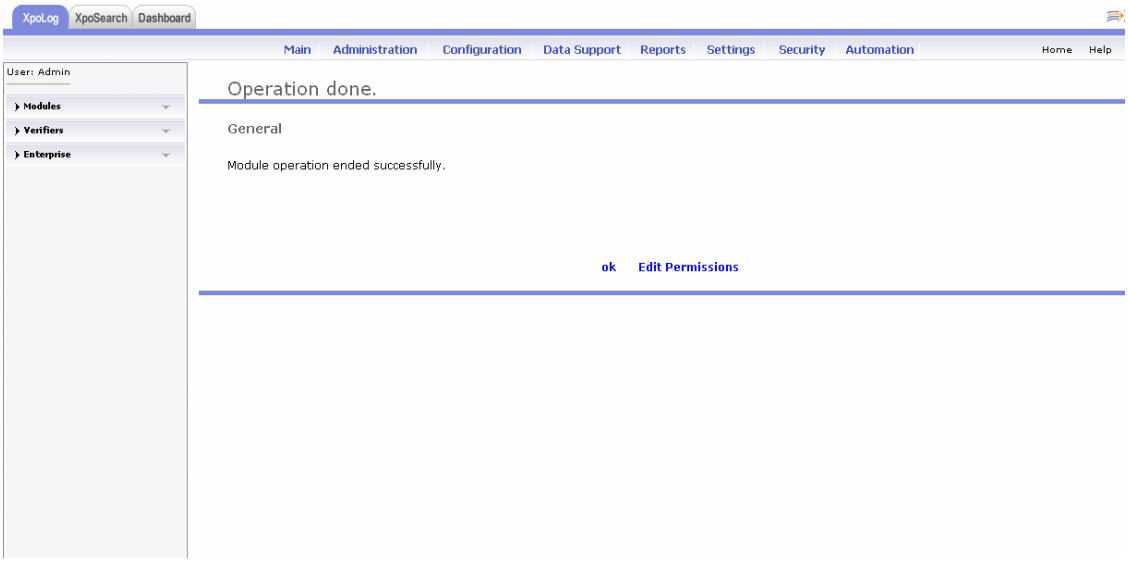
Module

- **Add module** – In order to add a new module, open the administration menu, and click 'Add module'. Select a parent module and add a module's name. You can add an owner and description for the module if desired. When finished, click 'Save'.

[1] Permission is presented only when Security is activated.

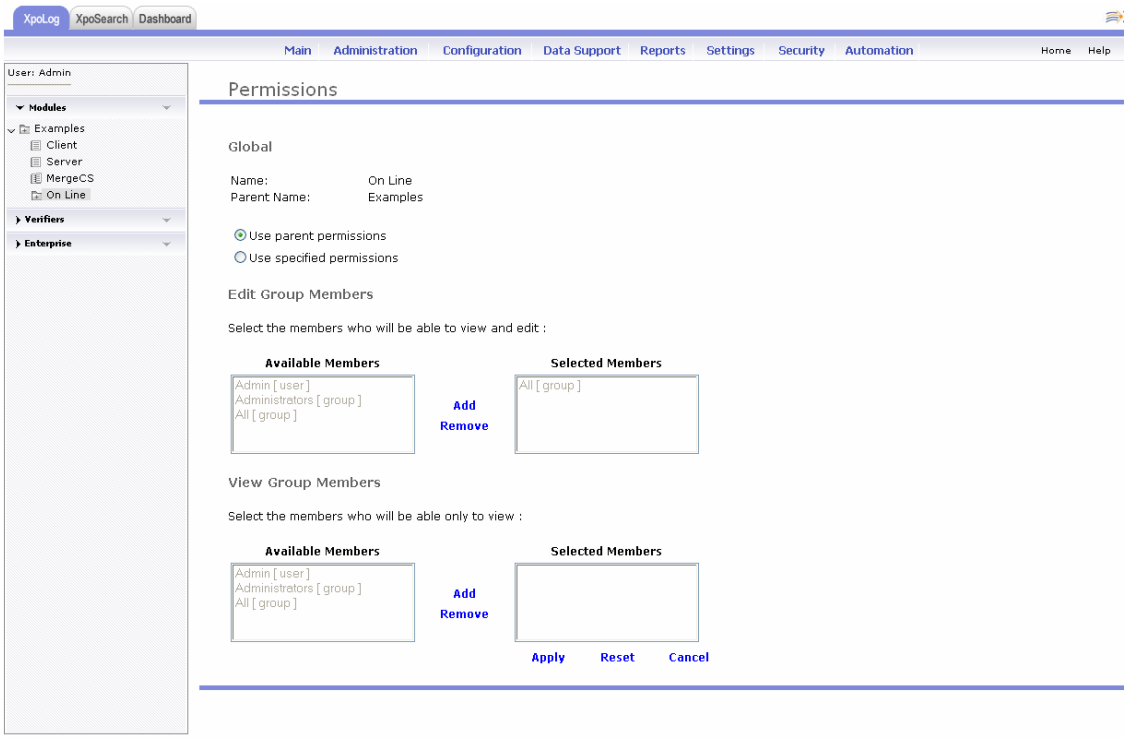


A message indicating that the operation ended successfully will be presented. Click ‘Ok’.



- **Edit module** – In order to edit an existing module via the administration menu, the specific module should be in focus. Select the relevant module in the left pane in the log viewer. When the module is in focus, open the administration menu and click ‘Edit module’. Edit the module’s properties and click save when done.
- **Edit module’s permissions** – Editing the module’s permissions enables you to set edit/view permissions for specific users/groups. . Editing the module’s permissions is only available when security is activated. For further information

on security, please refer to Settings → General. Open the administration menu, and click ‘Edit module permission’.

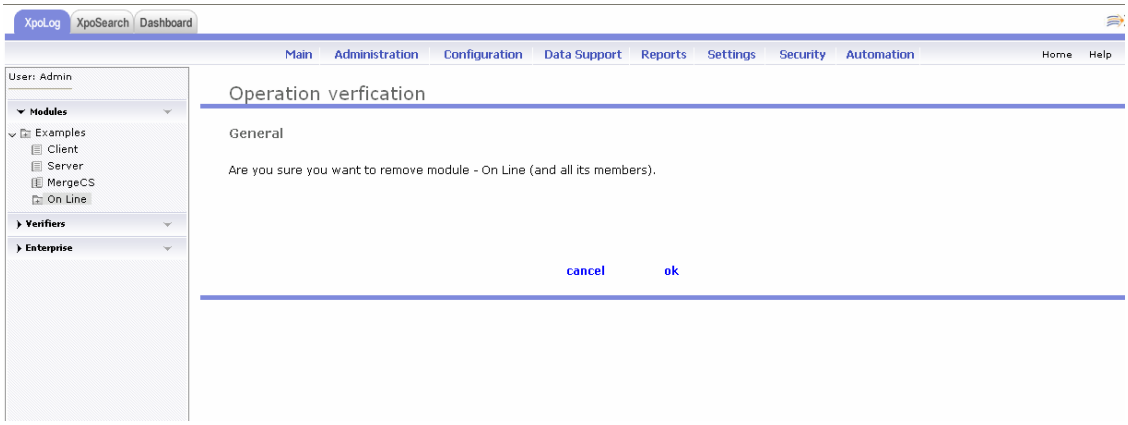


There are two options to set permissions:

1. ‘Parent permissions’ – this will set the same permissions as set in the parent module.
2. ‘Use specified permissions’ – selecting this option will allow you to add or remove users/groups from both available options: Edit group and the View group.

Click ‘Reset’ in case you would like to discard all changes, or click ‘Apply’ in order to save changes.

- **Edit module’s Meta data** – this option will be available only if module’s Meta data was added in advance. For further information, please go to Data support → Meta data.
- **Remove module** – in order to remove a module, open the administration menu, and click ‘Remove module’. Clicking ‘Ok’ will confirm deletion of module. In case you don’t want to delete it, click ‘Cancel’.

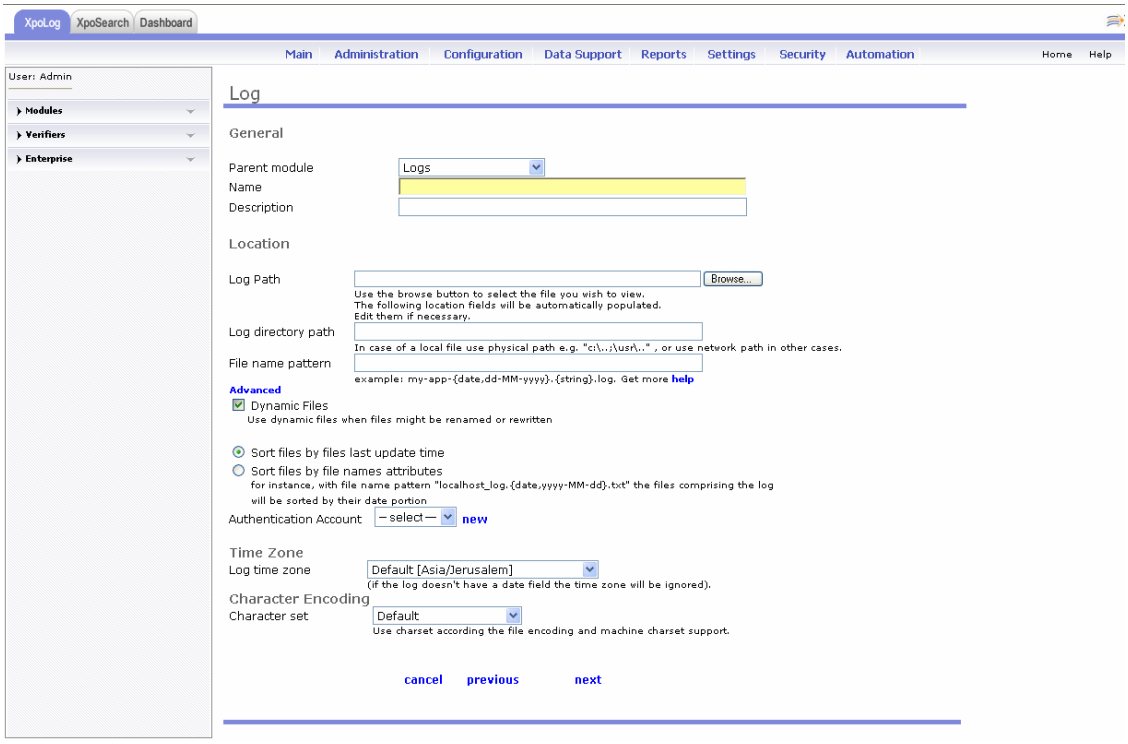

XpoLog
XpoSearch
Dashboard
Main
Administration
Configuration
Data Support
Reports
Settings
Security
Automation
Home
Help
User: Admin
Modules
Examples
Client
Server
MergeCS
On Line
Verifiers
Enterprise
Operation verfication
General
Are you sure you want to remove module - On Line (and all its members).
cancel
ok

Log

- **Add log** – In order to add a new log to XpoLog, open the administration menu and select 'Add log'. There are quite a few different logs that can be added to the XpoLog, in different methods.

The list of logs that can be added to the XpoLog

1. Manual configuration:



The first screen of the add log wizard

In order to manually add a regular log, select the manual configuration option. Select the parent module for this log, and configure the following General data: Name, Description.

Enter the log's path and the log directory path and file name pattern will be populated automatically. You can also configure the log directory path and the log's pattern directly.

Advanced - Dynamic files – Select this option in case the files might be renamed or overwritten.

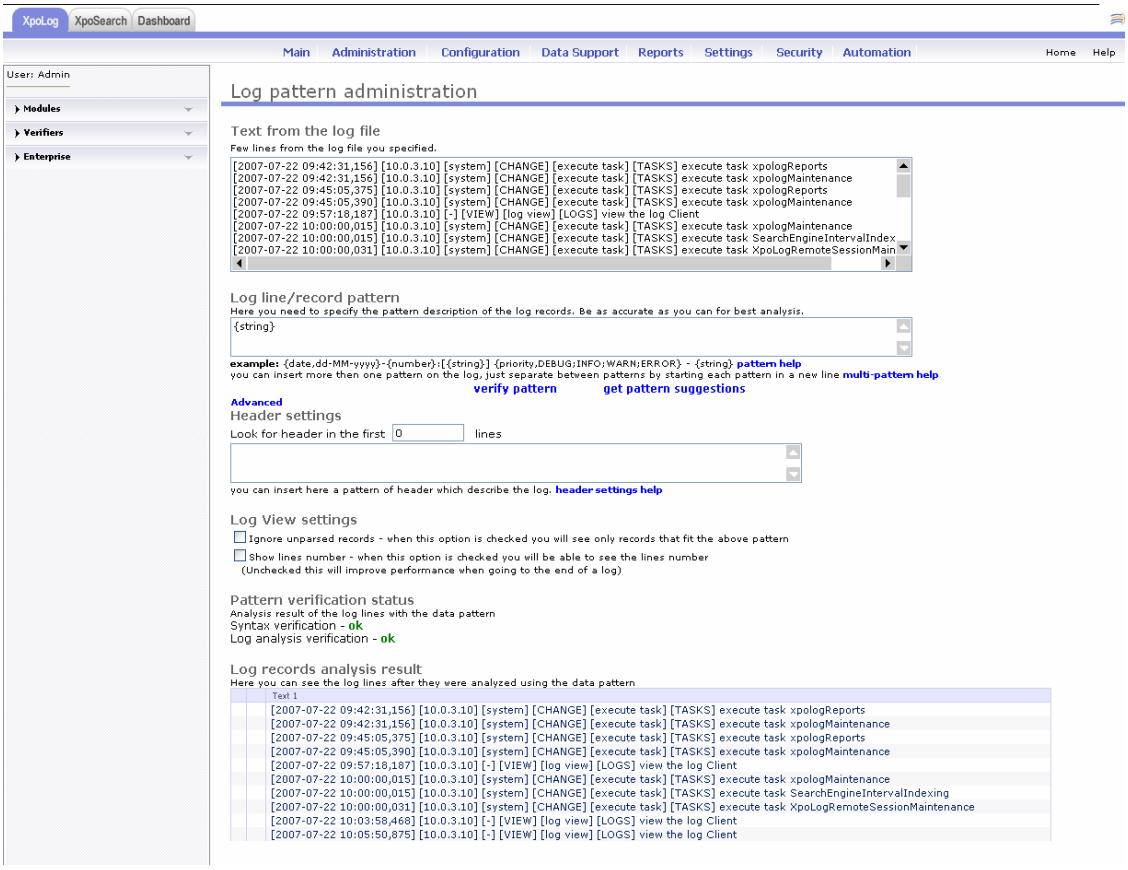
Sort files – Select the first option in order to sort files by date.

In case you would like to sort the files by names attributes, select the second option.

Authentication Account – select the appropriate account if one is needed to access files located on a remote machine.

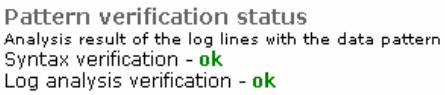
Moreover, it is possible to set the logs time zone as well as its character encoding. At this point you have two options: Click save, and skip the rest of the log wizard, or click next in order to continue configuring the log.

The next wizard screen is the log pattern administration:



The second screen of the add log wizard

A few lines from the log are presented in the ‘Text from the log file’ window. In the ‘Log line/Record pattern’ you need to add a pattern for the selected log. When done adding the desired pattern, click ‘Verify pattern’ to make sure that it was added correctly. The ‘pattern verification status’ will indicate whether the pattern is legal or not.



The ‘Log records analysis result’ will display a few lines from the parsed log.

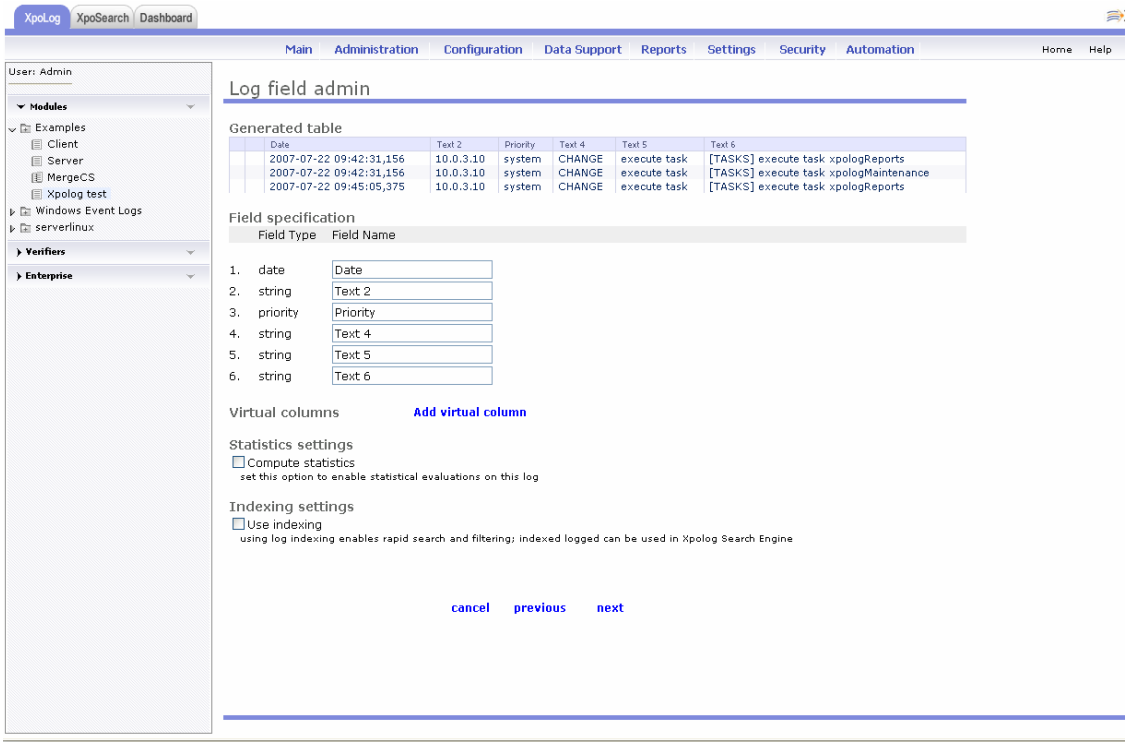
Header settings – set the number of lines according the log’s header length in case you wish XpoLog to disregard the log’s header.

You may add a separate pattern for the header as well.

Log view settings – Check the ‘Ignore unparsed records’ if you do not want XpoLog to show you records that does not match the log’s pattern. Check

the ‘Show line number’ in case you want to see the log’s line numbers (NOTE: This option will slow down XpoLog a bit).

Click next in order to move on to the last screen of the log’s wizard:

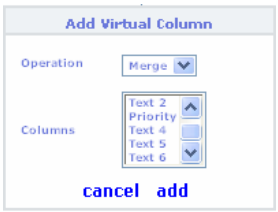


The third screen of the add log wizard

In this screen you can set the columns name, add a virtual column and set the statistics/indexing settings.

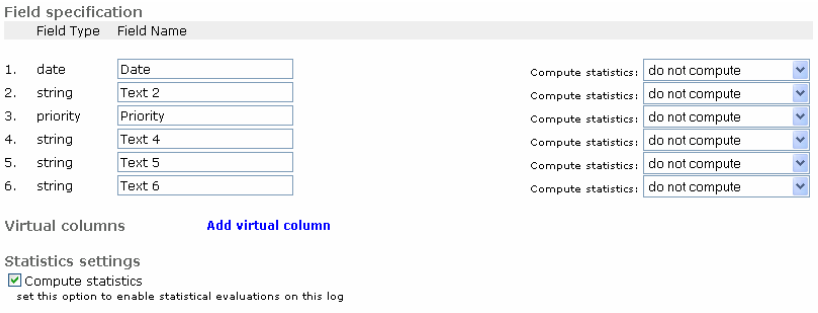
Rename columns – in the field name, enter the desired column name.

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.



The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.

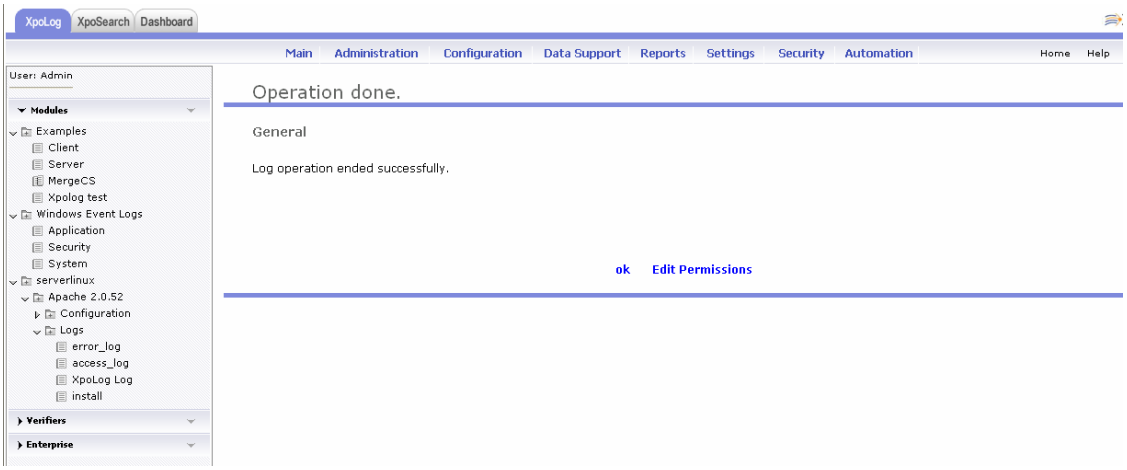


Statistical computation settings can be applied to each column separately

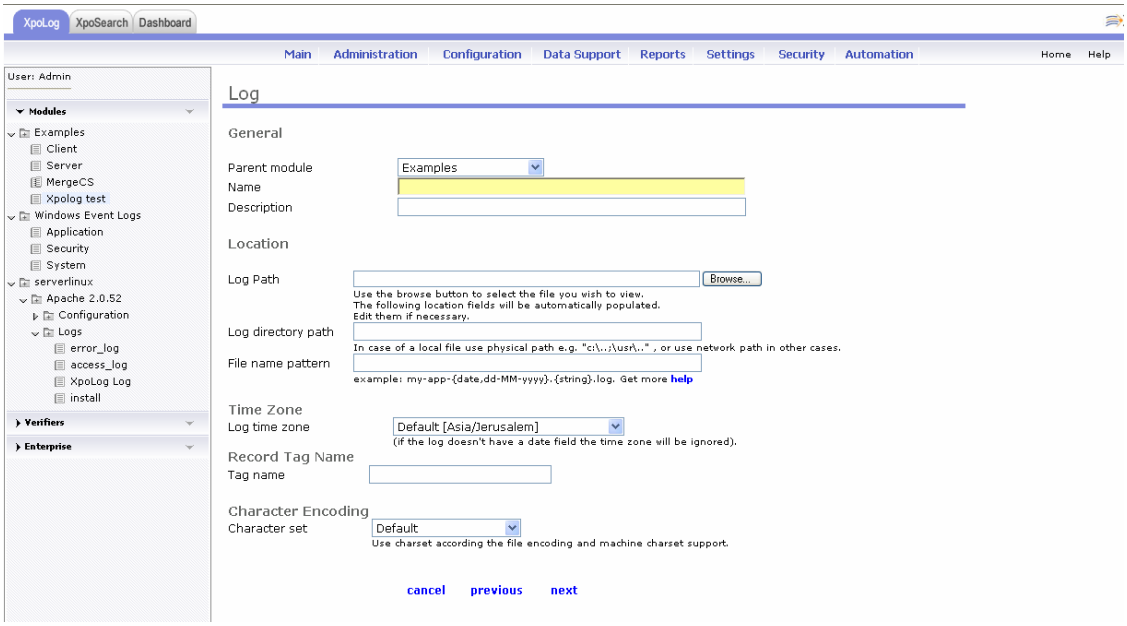
Indexing setting: check the 'Use indexing' in order to index the log. When the 'use indexing' is marked, a second indexing option appears: 'Use indexing for date search'. For further information, please refer to XpoSearch.

When done configuring the indexing, click 'Next'.

The log's wizard is done; Click OK to end the wizard. In case security is activated, you may edit the log's permissions by clicking 'Edit Permissions'.



2. <u>Manual XML log configuration:</u>



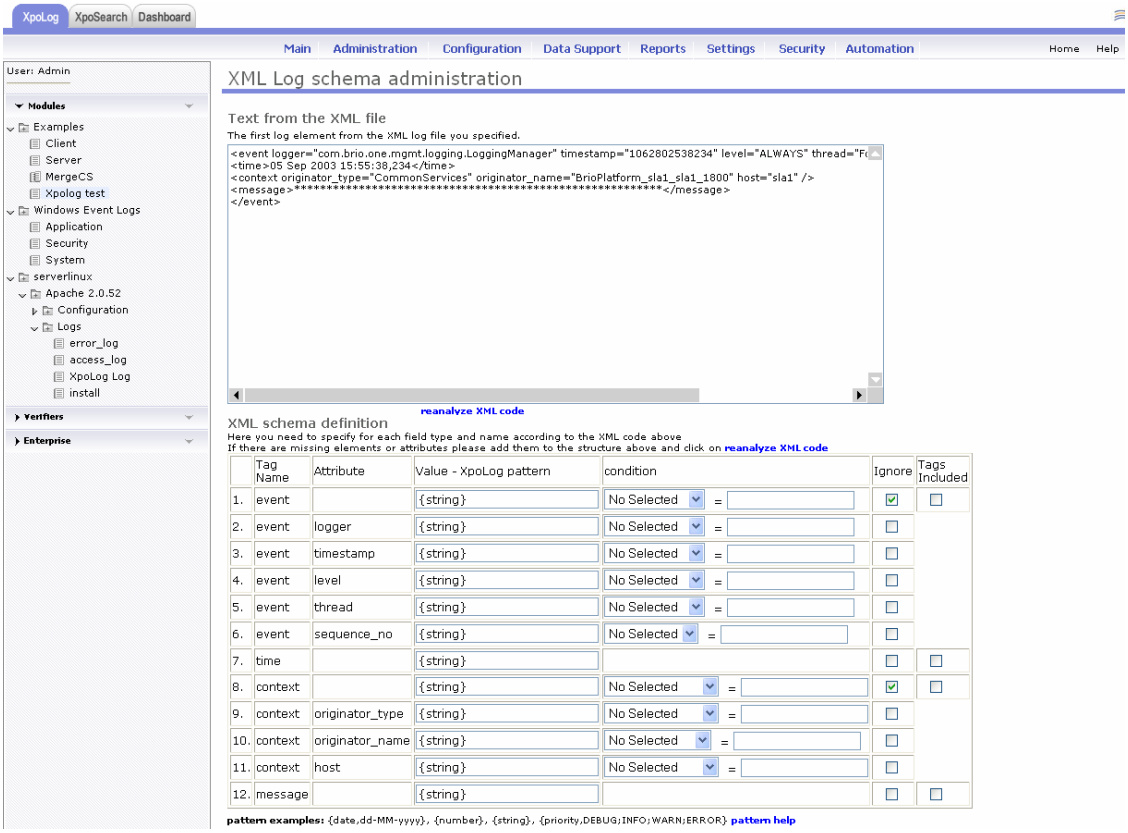
In order to add an XML log, select the manual XML log configuration option. Select the parent module for this log, and configure the following General data: Name, Description.

Enter the log's path and the log directory path and file name pattern will be populated automatically. You can also configure the log directory path and the log's pattern directly.

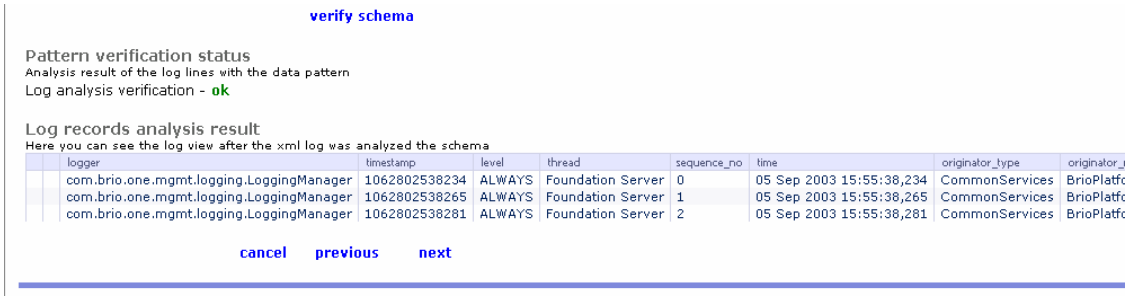
Set the logs time zone, the record tag name and the character encoding.

Click next in order to continue configuring the log.

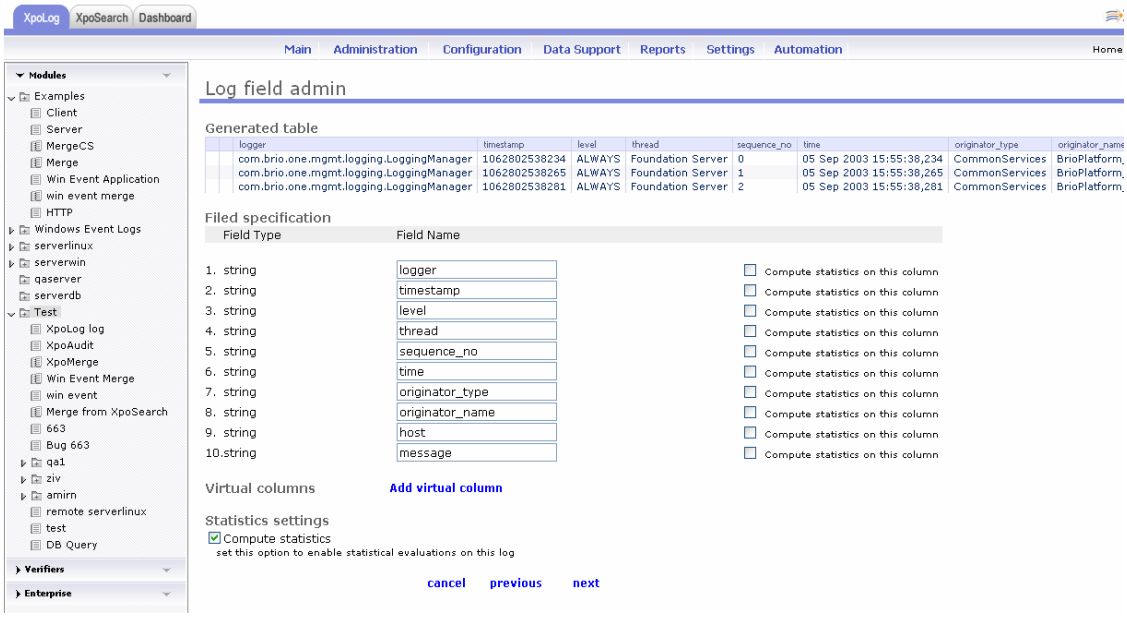
In the second wizard's screen you will need to configure the XML log schema by specifying for each field type and name a pattern and a condition according to the XML code above. If there are missing elements or attributes please add them to the structure above and click the 'Reanalyze XML code'.



Use the ‘Verify Schema’ to see a preview of the analyzed log according to the given pattern.

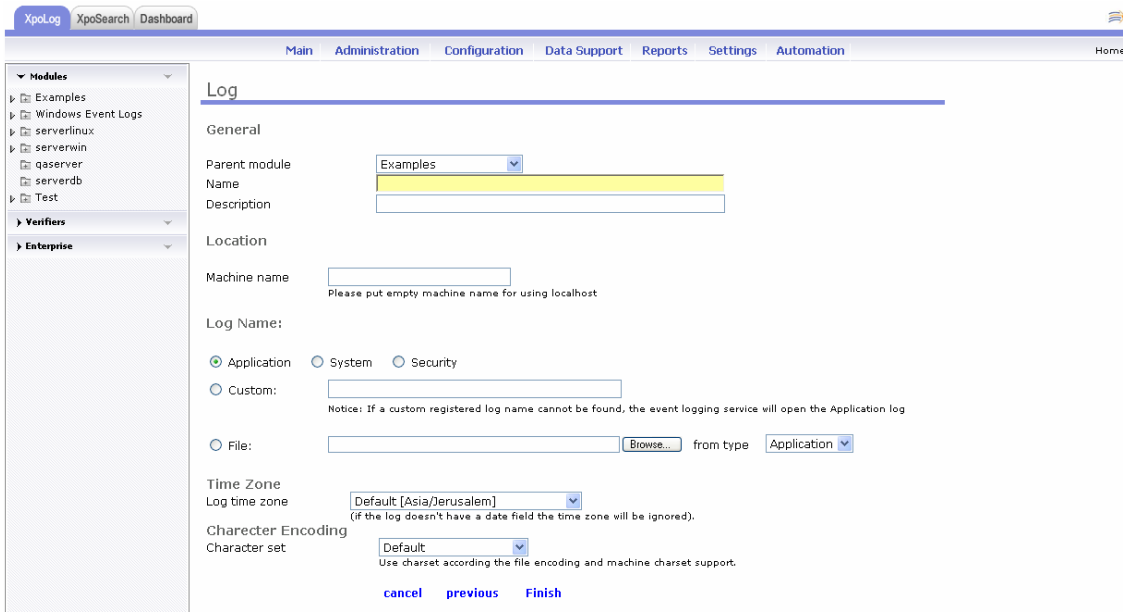


Click ‘next’ to move on to the last wizard’s screen, where you will have to configure the field specification, virtual columns and statistics computation.



Click ‘next’ in order to finish the log’s wizard. You may also go back, using the ‘previous’ link, and reconfigure the log’s properties.

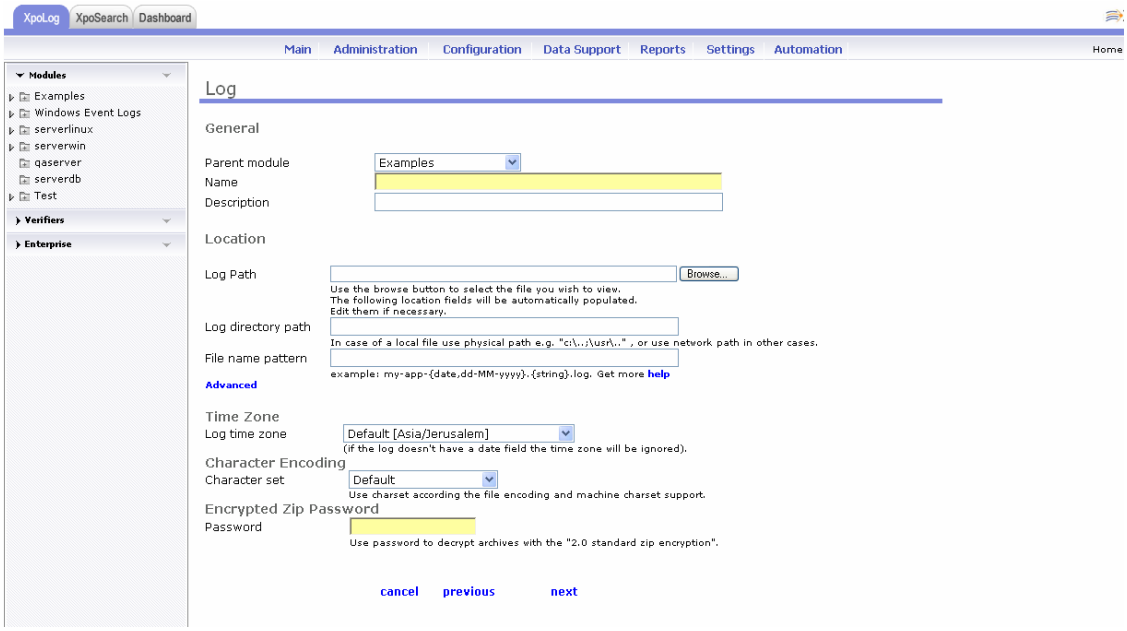
3. <u>Windows events log:</u>



In order to add a Windows event log, select the ‘Windows event log’ configuration option. Select the parent module for this log, and configure the following General data: Name and Description.

Enter the machine name, or leave it empty in case the logs are located in localhost. Specify the log type: Application, System or Security.
A different option would be select ‘File’ and add the relevant path manually along with the log’s type.
Set the logs time zone and the character encoding.
When done configuring the Windows event log, click ‘Finish’ to exit the wizard.

4. Encrypted text zip archive:

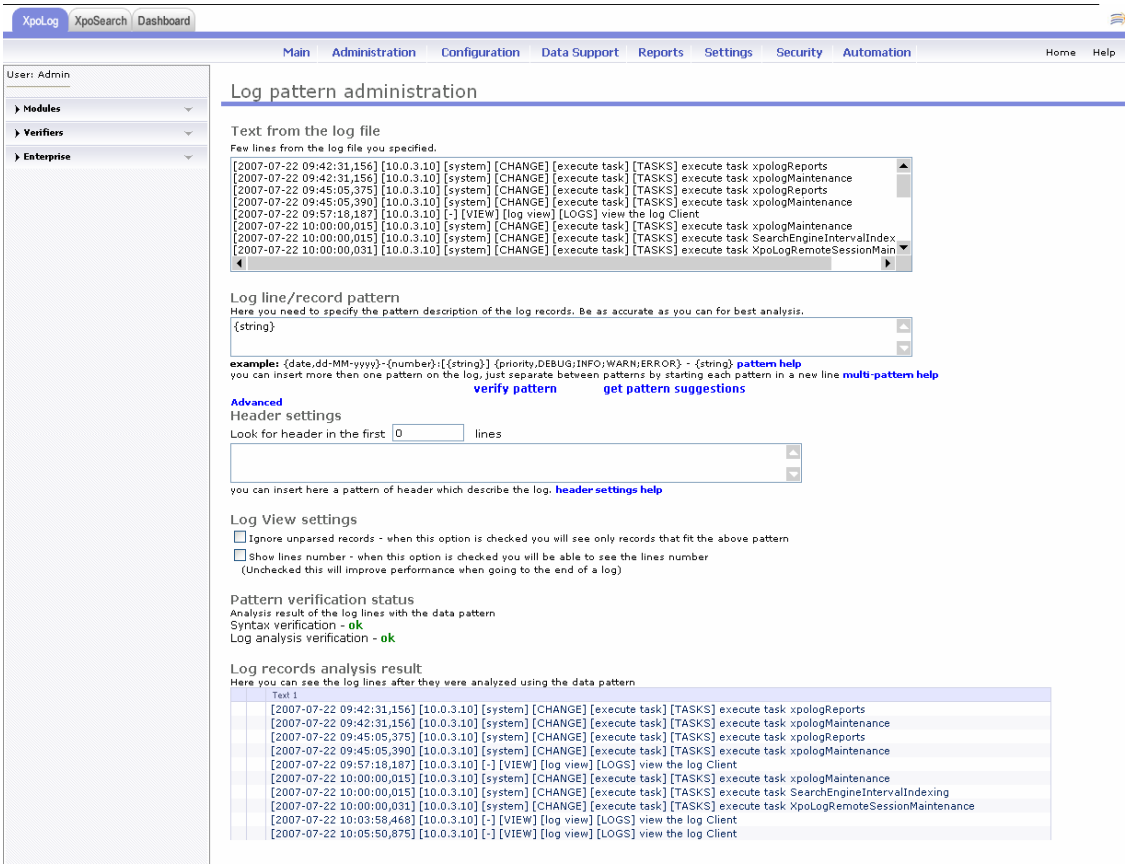


In order to manually add an encrypted zip log, select the ‘Encrypted text zip archive’ option. Select the parent module for this log, and configure the following General data: Name, Description.
Enter the log’s path and the log directory path and file name pattern will be populated automatically. You can also configure the log directory path and the log’s pattern directly.
Advanced - Dynamic files – Select this option in case the files might be renamed or overwritten.
Sort files – Select the first option in order to sort files by date.
In case you would like to sort the files by names attributes, select the second option.

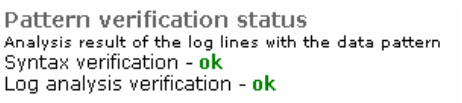
Authentication Account – select the appropriate account if one is needed to access files located on a remote machine.

Moreover, it is possible to set the logs time zone as well as its character encoding. Finally, add the encrypted zip password.

Click next in order to continue to the next wizard's screen.



A few lines from the log are presented in the 'Text from the log file' window. In the 'Log line/Record pattern' you need to add a pattern for the selected log. When done adding the desired pattern, click 'Verify pattern' to make sure that it was added correctly. The 'pattern verification status' will indicate whether the pattern is legal or not.



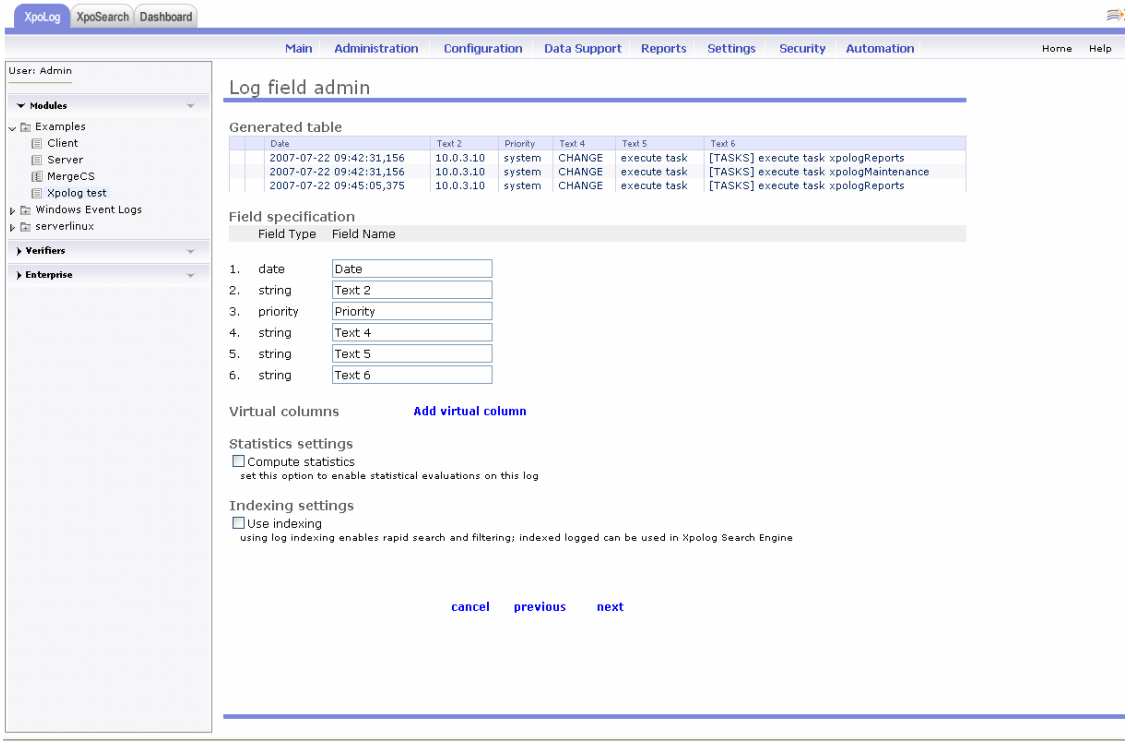
The 'Log records analysis result' will display a few lines from the parsed log.

Header settings – set the number of lines according the log's header length in case you wish XpoLog to disregard the log's header.

You may add a separate pattern for the header as well.

Log view settings – Check the ‘Ignore unparsed records’ if you do not want XpoLog to show you records that does not match the log’s pattern. Check the ‘Show line number’ in case you want to see the log’s line numbers (NOTE: This option will slow down XpoLog a bit).

Click next in order to move on to the last screen of the log’s wizard:

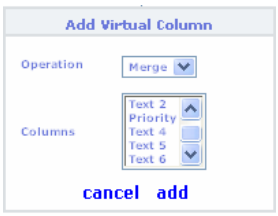


The third screen of the add log wizard

In this screen you can set the columns name, add a virtual column and set the statistics/indexing settings.

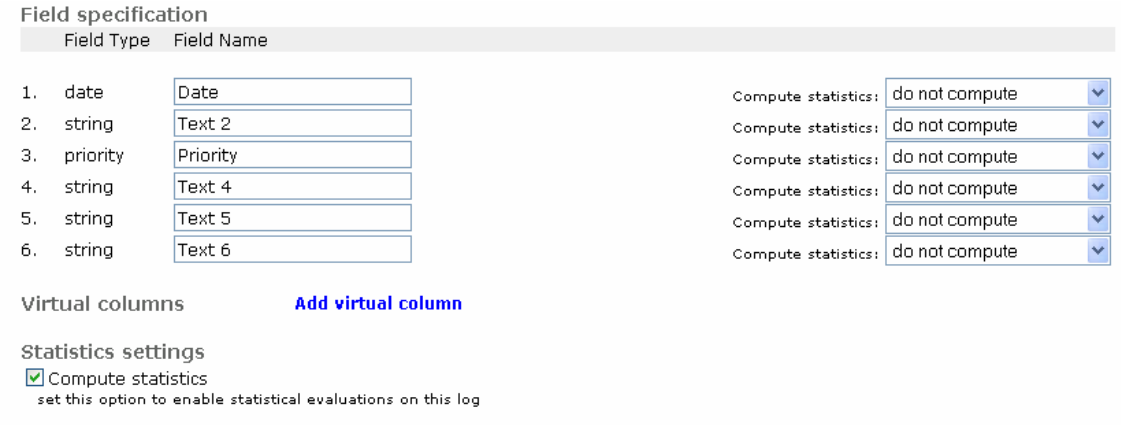
Rename columns – in the field name, enter the desired column name.

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.



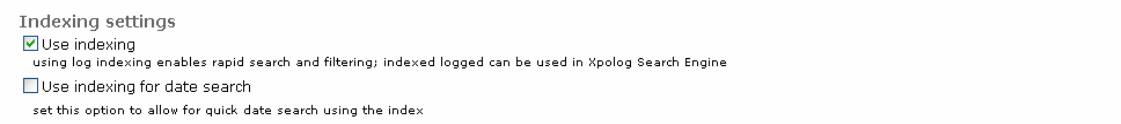
The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.



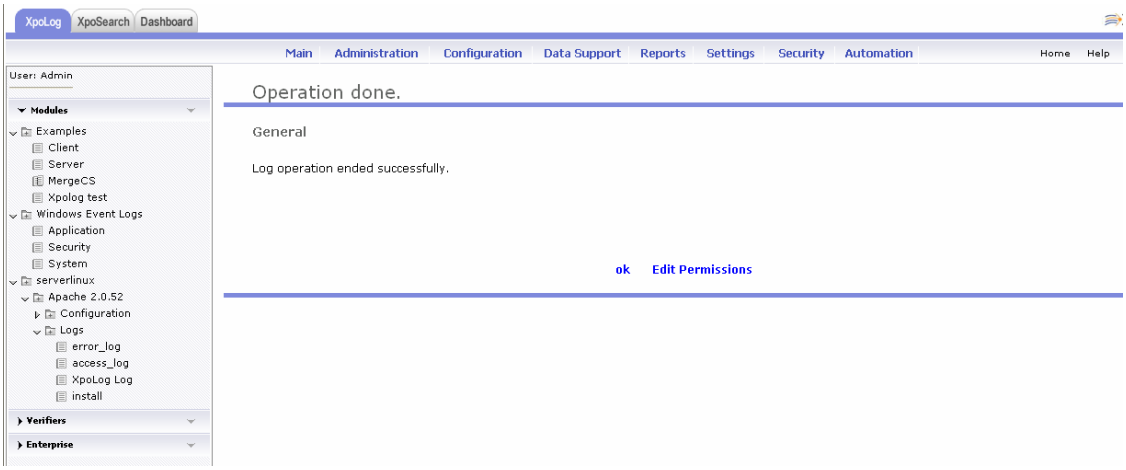
Statistical computation settings can be applied to each column separately

Indexing setting: check the ‘Use indexing’ in order to index the log. When the ‘use indexing’ is marked, a second indexing option appears: ‘Use indexing for date search’. For further information, please refer to XpoSearch.

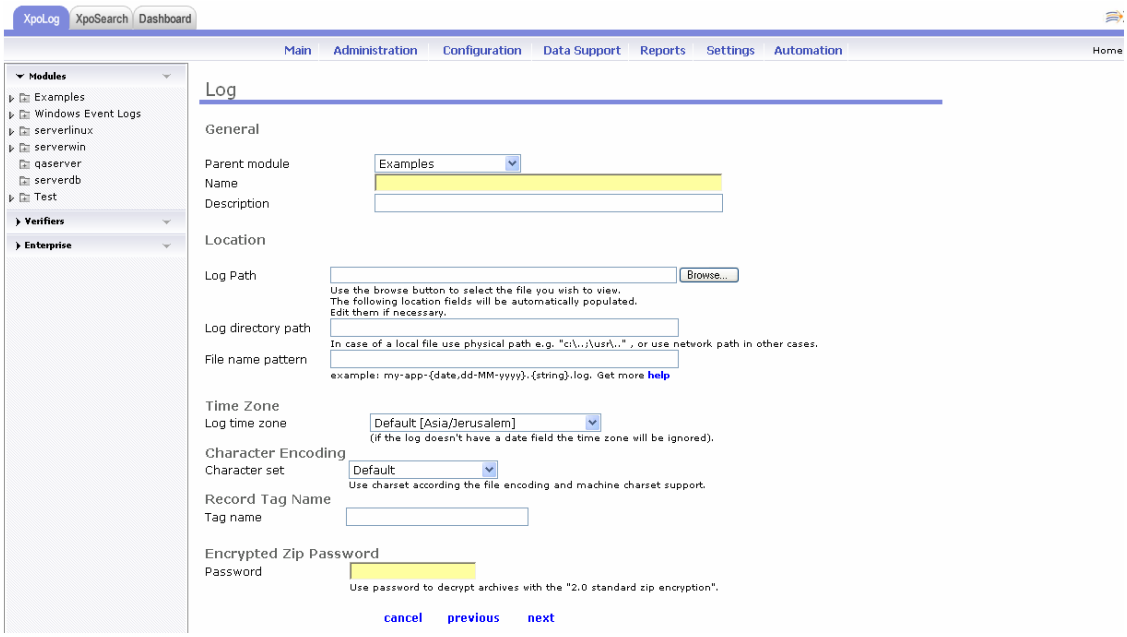


When done configuring the indexing, click ‘Next’.

The log’s wizard is done; Click OK to end the wizard. In case security is activated, you may edit the log’s permissions by clicking ‘Edit Permissions’.



5. Encrypted XML zip archive:



In order to add an encrypted XML log, select the ‘encrypted XML zip archive’ option. Select the parent module for this log, and configure the following General data: Name, Description.

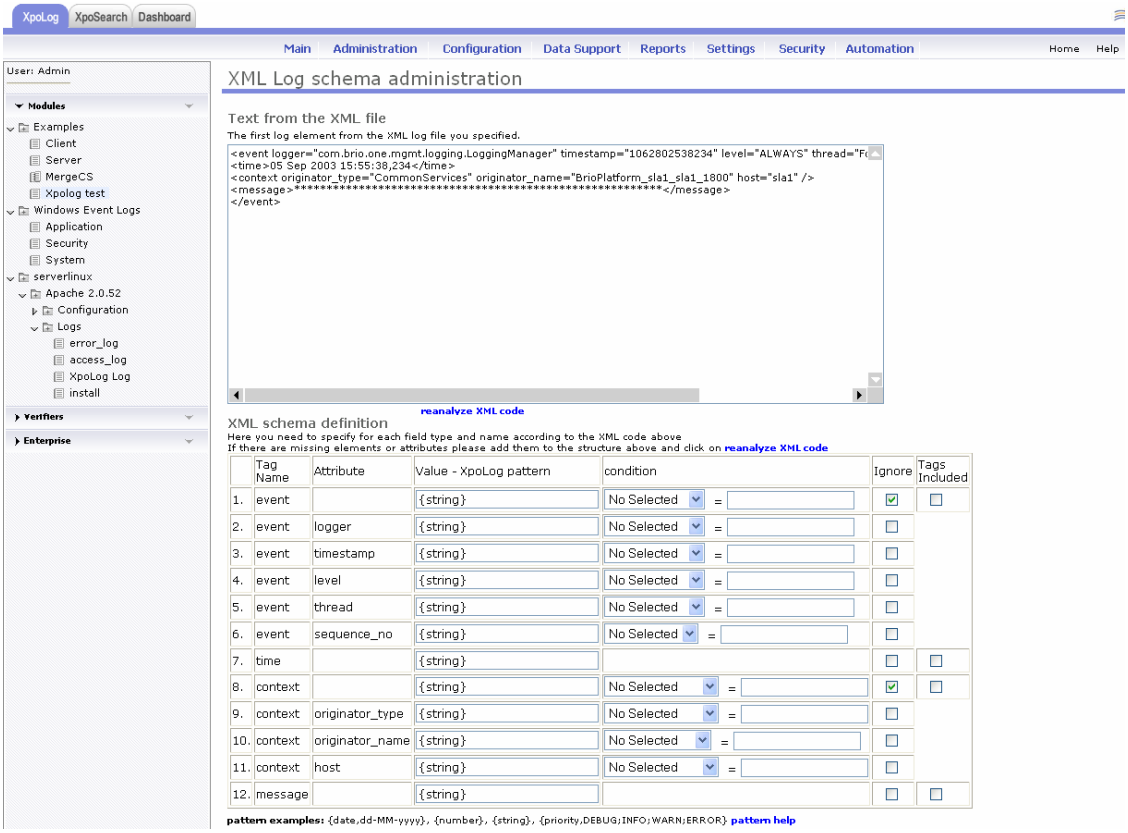
Enter the log’s path and the log directory path and file name pattern will be populated automatically. You can also configure the log directory path and the log’s pattern directly.

Set the logs time zone, and the character encoding.

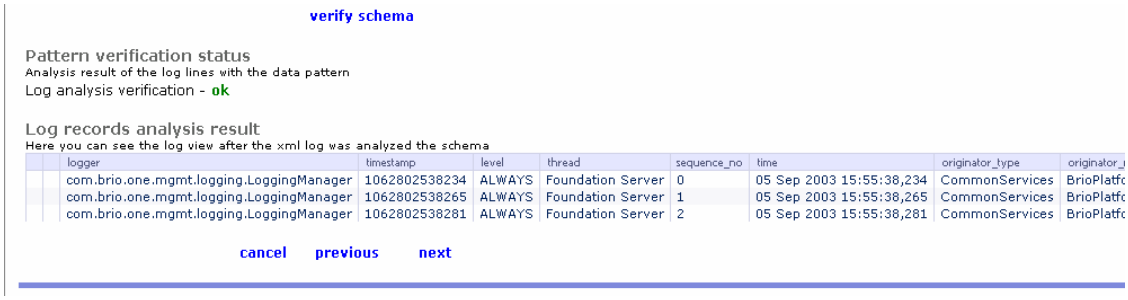
Enter the record tag name

Click next in order to continue configuring the log.

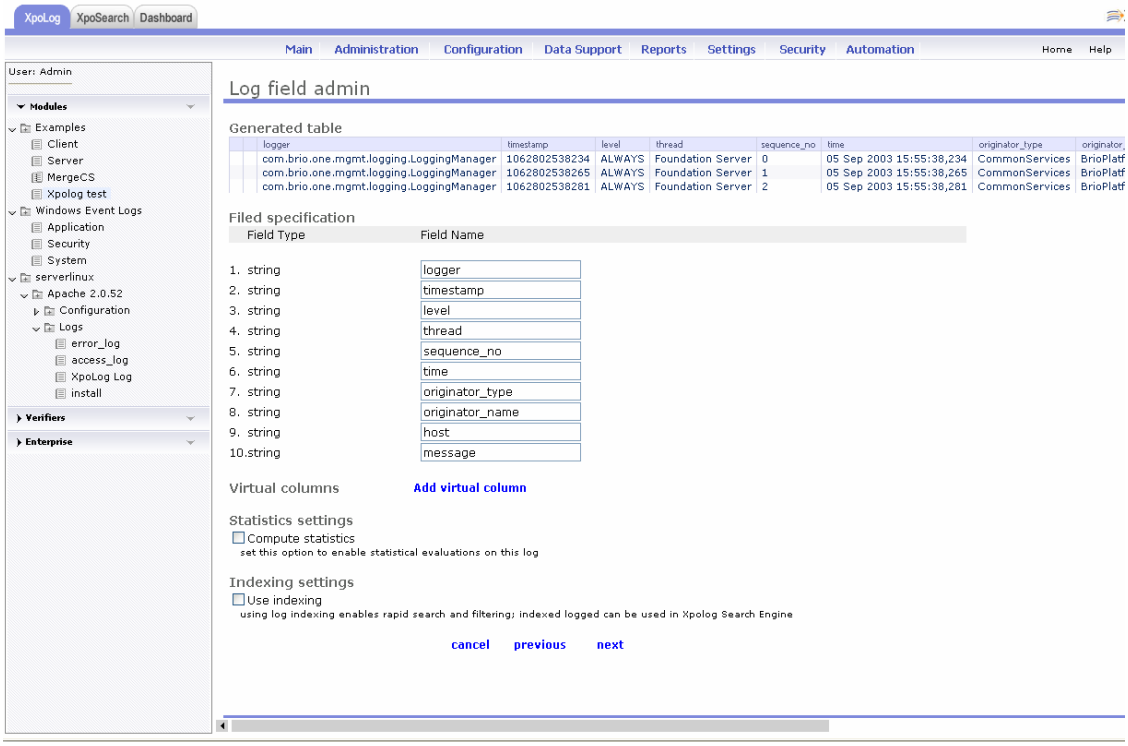
In the second wizard’s screen you will need to configure the XML log schema by specifying for each field type and name a pattern and a condition according to the XML code above. If there are missing elements or attributes please add them to the structure above and click the ‘Reanalyze XML code’.



Use the ‘Verify Schema’ to see a preview of the analyzed log according to the given pattern.



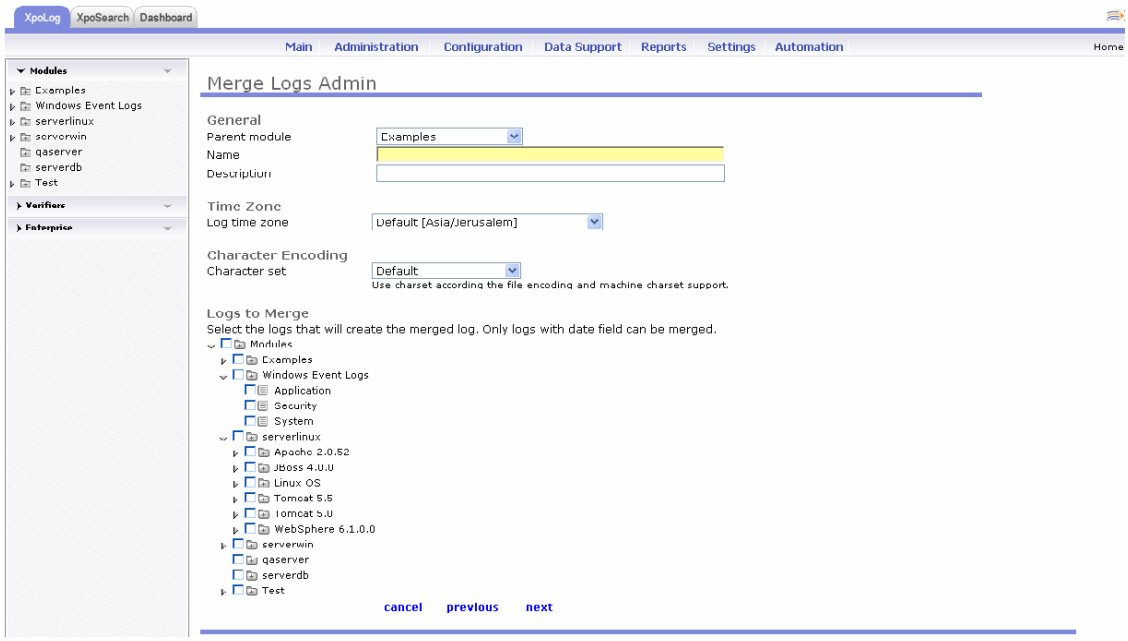
Click ‘next’ to move on to the last wizard’s screen, where you will have to configure the field specification, virtual columns, statistics computation and the use of indexing.



Click ‘next’ in order to finish the log’s wizard. You may also go back, using the ‘previous’ link, and reconfigure the log’s properties.

6. <u>Merge logs:</u>

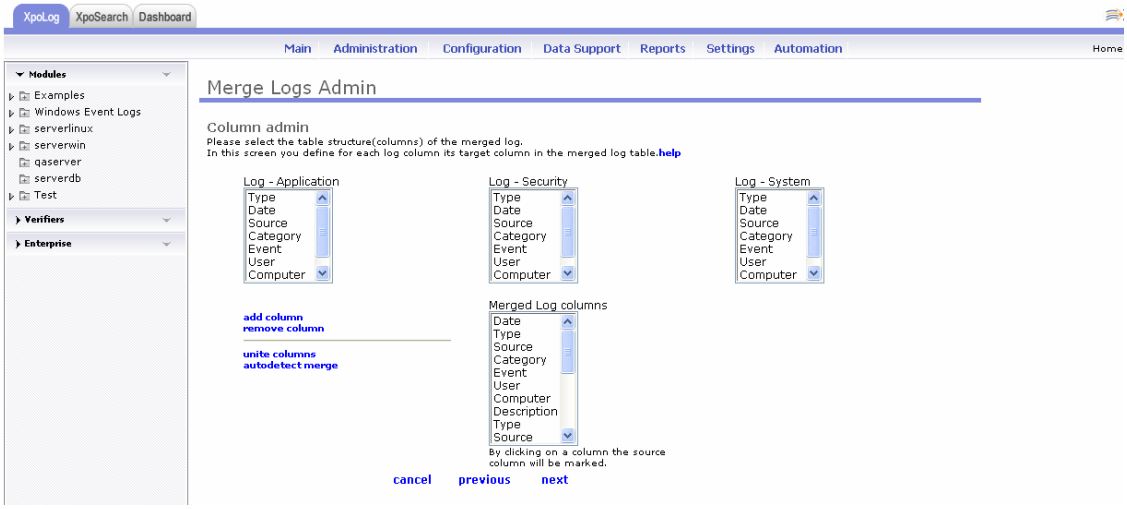
   The merge logs feature allows the merge of two or more predefined logs into a single log.



In the wizard, configure the general data: Parent module,

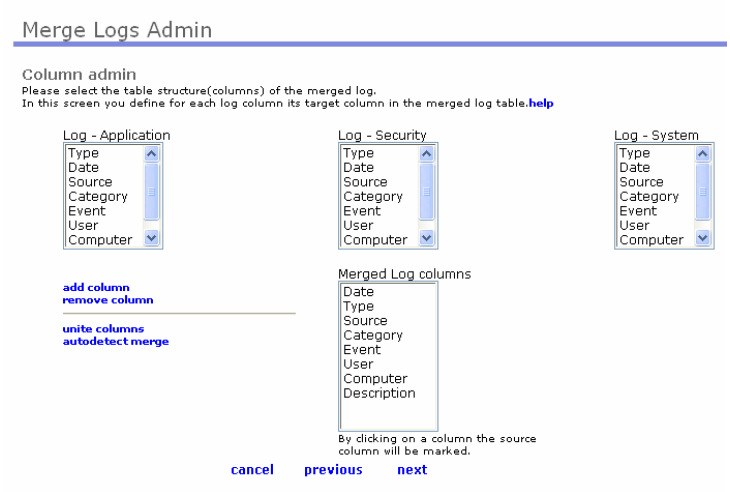
name, description, logs time zone and the character encoding.

Logs to merge – Select the logs you would like to merge from the list of available logs in XpoLog, and click ‘next’.



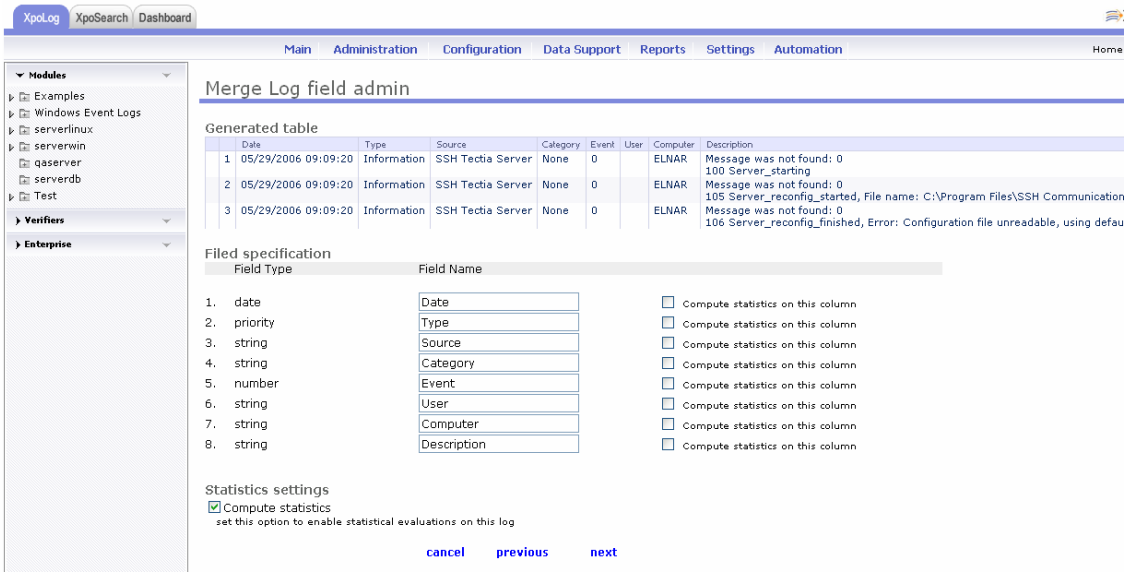
In this screen you are configuring the merged log columns by adding columns from the source logs. XpoLog can auto detect similar columns from different source logs and unite them in the merged log.

Click the ‘Auto detect merge’ in order to activate this operation



The merge logs admin after auto-detection

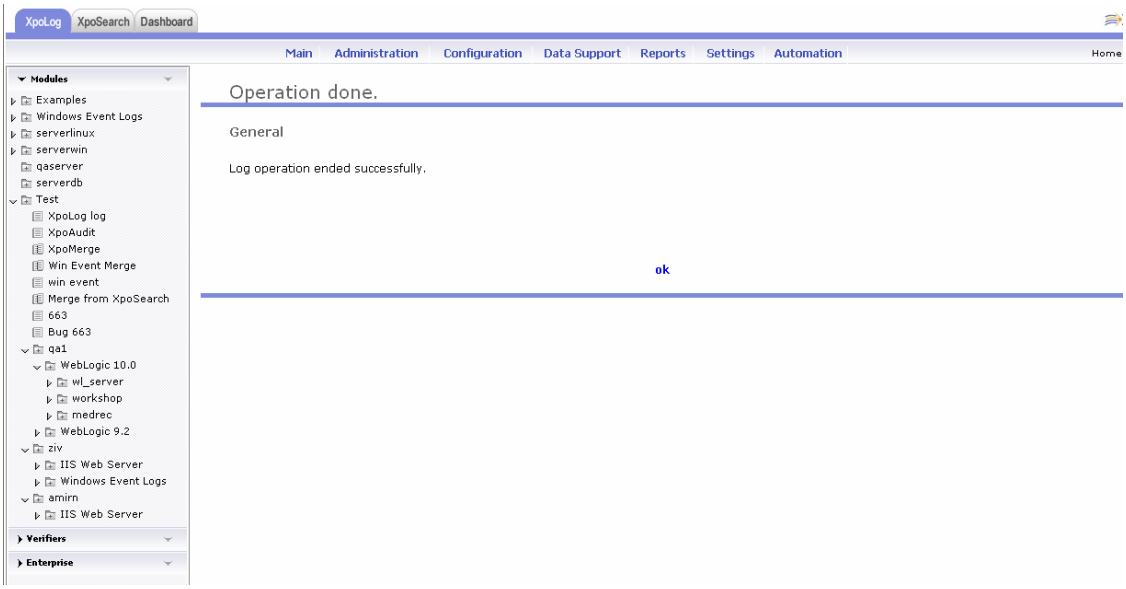
Click ‘Next’ in order to move on to the last merge log’s configuration screen.



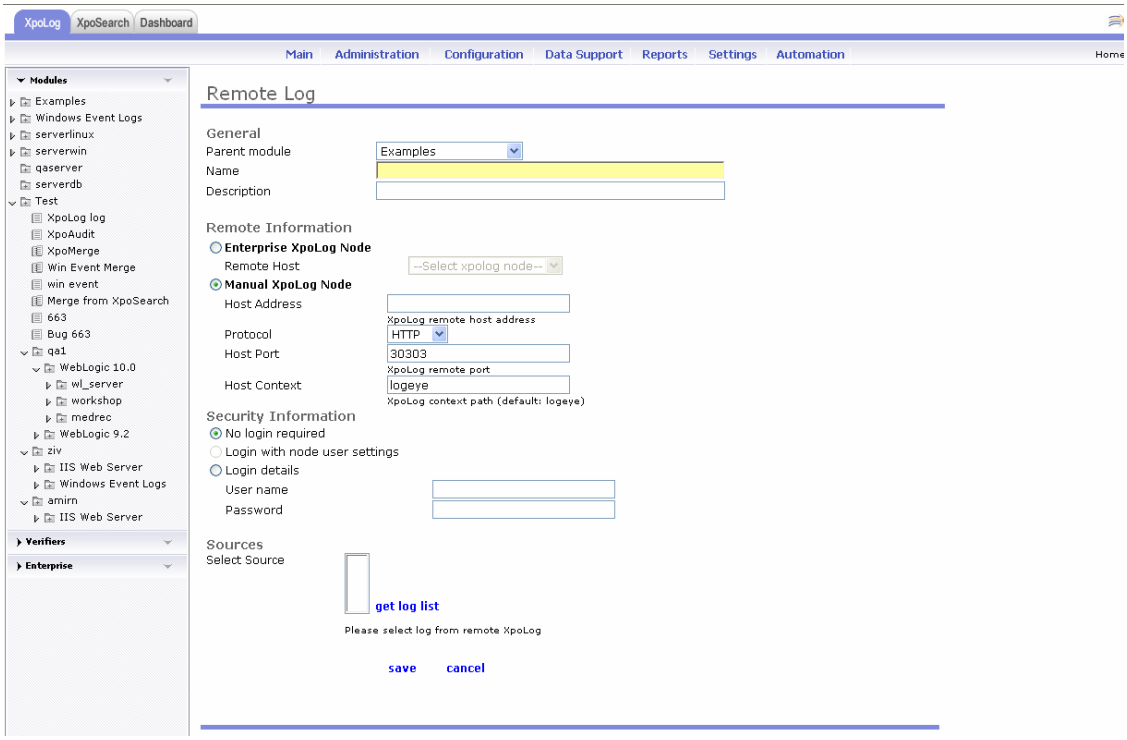
In this screen you can see a short preview of the merged log (Generated table), and rename any of the fields name.

Moreover, you can select whether you would like XpoLog to compute statistics for the new merged log. Hence that XpoLog cannot run indexing on merged logs.

Click next, and confirm the successful creation of the merged log.



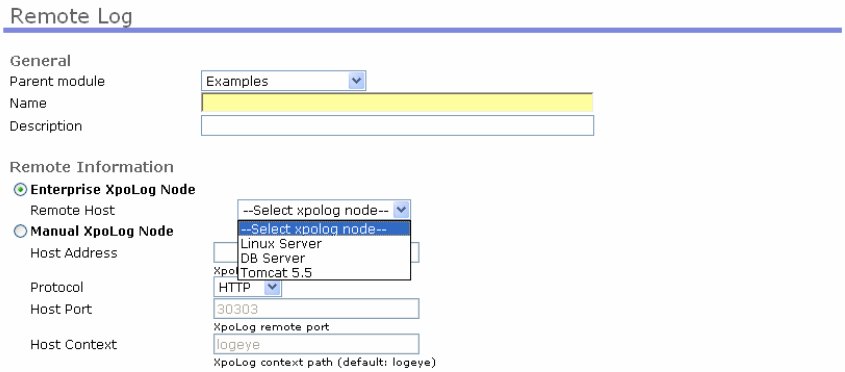
7. Remote XpoLogs:



XpoLog allows you to add logs from remote XpoLogs.

Select a parent module, log name and description.

Select whether you would like to select an XpoLog node from a list of available nodes, or add one manually. A list of existing XpoLog nodes will be displayed in case such nodes were configured beforehand. For further information regarding XpoLog nodes, please refer to Data Support → Enterprise.



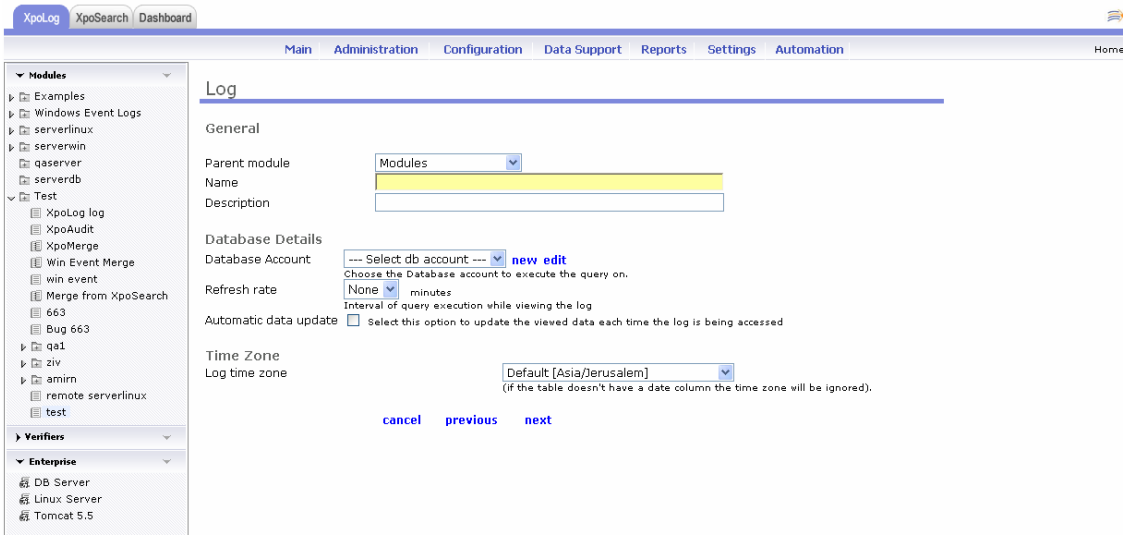
The list of predefined XpoLog nodes

In order to manually add an XpoLog node, select 'Manual XpoLog Node' and set the host address, Protocol, and the host's port.

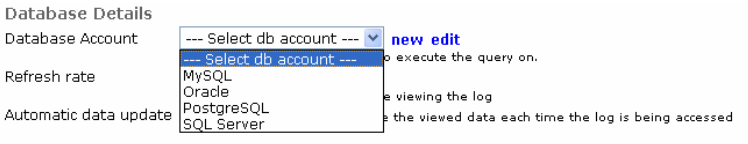
In case security is activated at the remote XpoLog node, select the ‘Login details’ and provide a valid user name and password. If the security is inactive, you can leave the ‘No login required’ option selected.
Clicking the ‘get log list’ will display all logs available in the remote XpoLog.

Select the log you wish to add to XpoLog and click ‘Save’.

8. <u>Data Base query:</u>



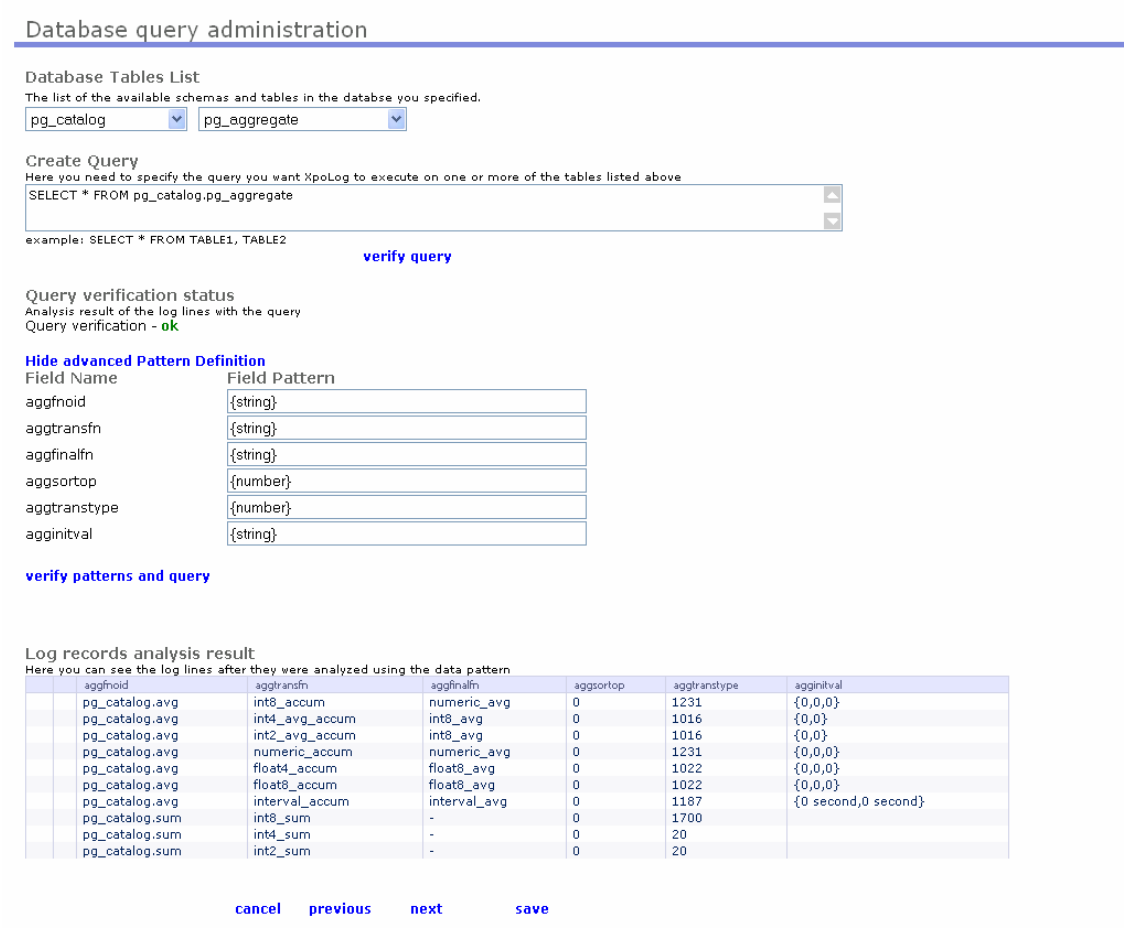
The database query log feature allows you to create a log based upon a DB query. In the log wizard, select a parent module, log name and description.
DB details – Select a DB account from the combo box:



Click ‘new’ in order to create a new DB account, or click ‘edit’ in order to edit an existing one. For further information on DB accounts, please refer to data support – database.
Select the ‘refresh rate’ time in minutes.
Selecting ‘Automatic data update’ will automatically update the existing data every time the log is accessed.

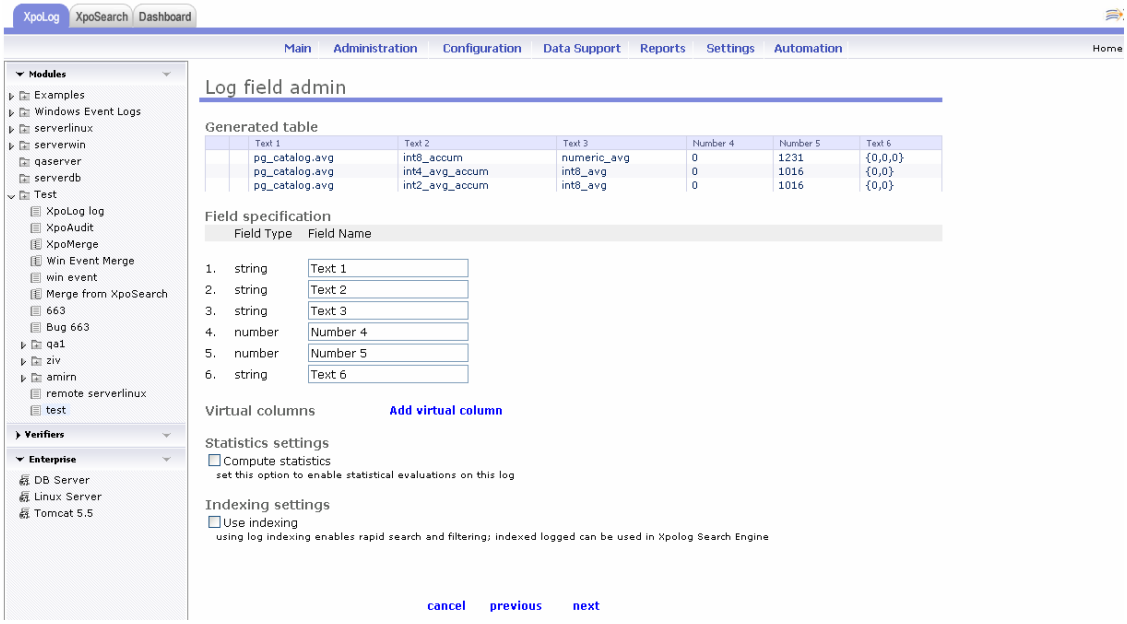
Click ‘next’ in order to continue configuring the log.

From the database tables list select the desired schema and table available according to the DB specified.



In the create query field you need to specify the query XpoLog should execute on the tables selected.

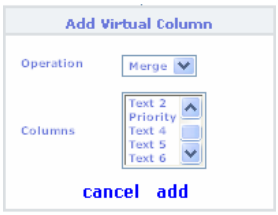
You may also change the field pattern in the advanced pattern definition. Click ‘verify query’ or ‘verify patterns and query’ to confirm it is correct. XpoLog will display a few records from the analyzed data in the ‘log records analysis’ table. Click ‘next’ in order to continue the log’s configuration or click ‘save’ if you are finished configuring.



‘Generated table’ is an example of how the log will look like.

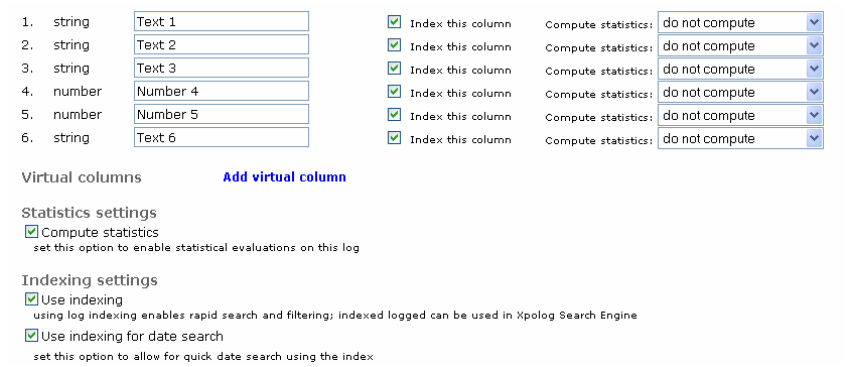
In the ‘field specification’ you may change the field name of each of the columns.

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.



The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.



Statistical computation and Indexing settings can be applied to each column separately

Indexing setting: check the 'Use indexing' in order to index the log.

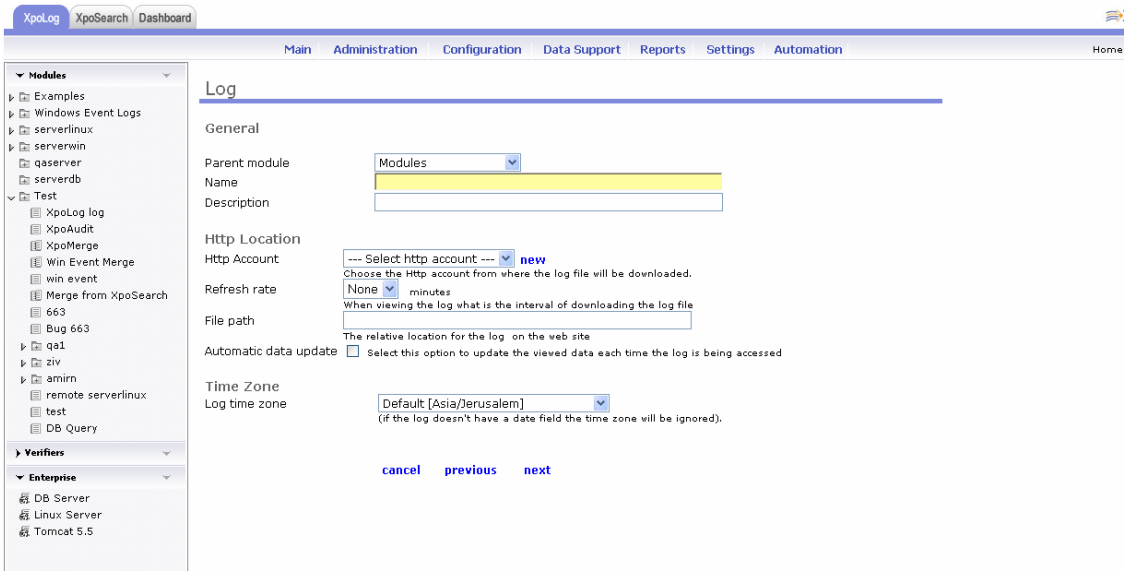
You may select statistics computation for each and every column separately.

When the 'use indexing' is marked, a second indexing option appears: 'Use indexing for date search'. For further information, please refer to XpoSearch.

Click 'Next' in order to finish and save the log's wizard.

The log wizard ended successfully. Click 'ok' to confirm operation.

9. <u>Add HTTP log configuration:</u>



You can create an HTTP log in XpoLog. From the data source administration, select ‘Add HTTP log configuration’.

Select the parent module for this log, and specify name and description.

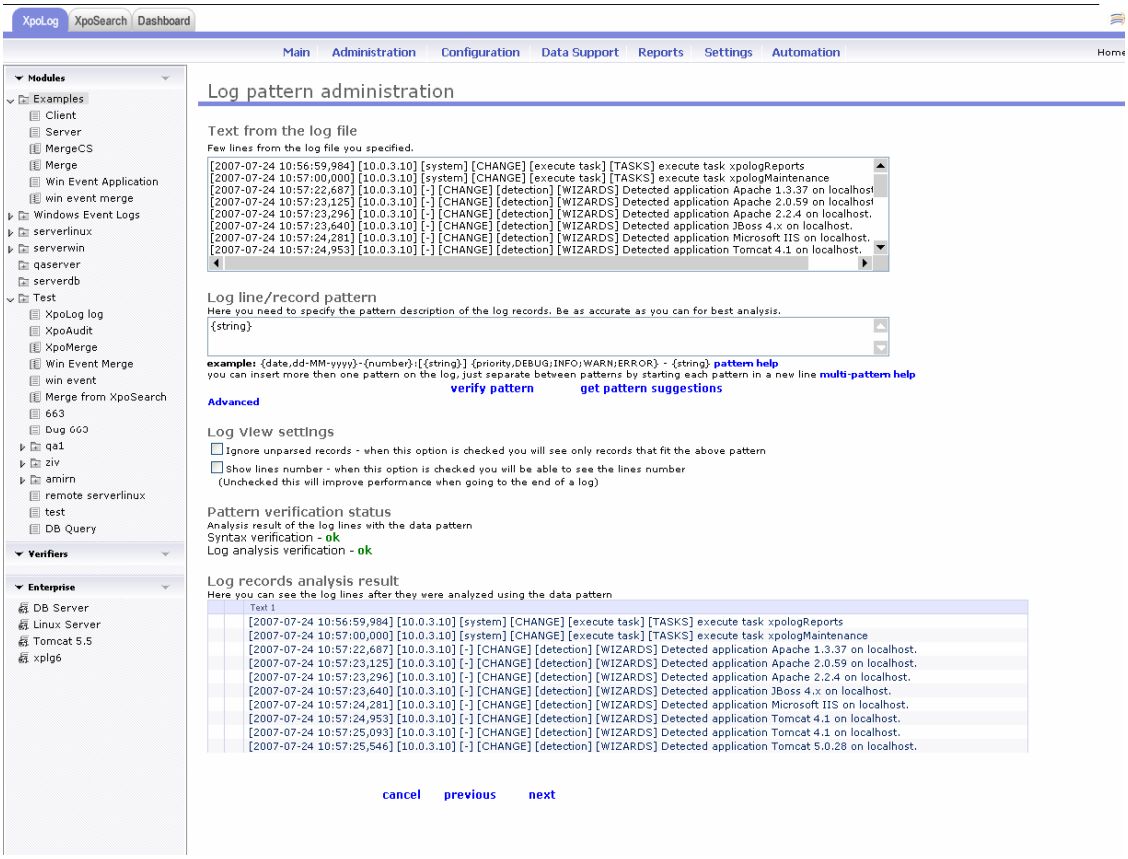
Select the relevant HTTP account for this log from the list of available accounts, or create a new HTTP account by clicking ‘new’. For further information on HTTP accounts, please refer to Data Support → Address book → HTTP.

Select the refresh rate in minutes for XpoLog to download the log file.

In the ‘file path’, you should supply the log’s relative path in the web site.

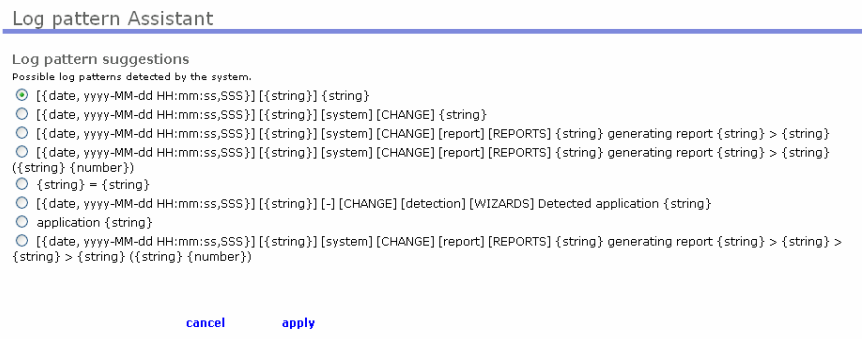
Selecting ‘Automatic data update’ will automatically update the existing data every time the log is accessed.

Select the log’s time zone, and click ‘next’ in order to continue the log’s configuration.



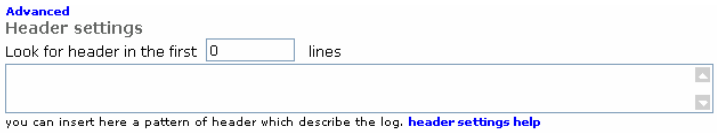
The ‘Text from the log file’ is a short preview of the log specified.

In the log line/record pattern specify a pattern according to the way you would like XpoLog to analyze the log. Click on the ‘get pattern suggestions’ and a few basic pattern alternatives to choose from, will be displayed.

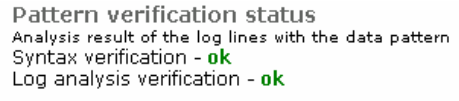


Header settings – set the number of lines according the log’s header length in case you wish XpoLog to disregard the log’s header.

You may add a separate pattern for the header as well.



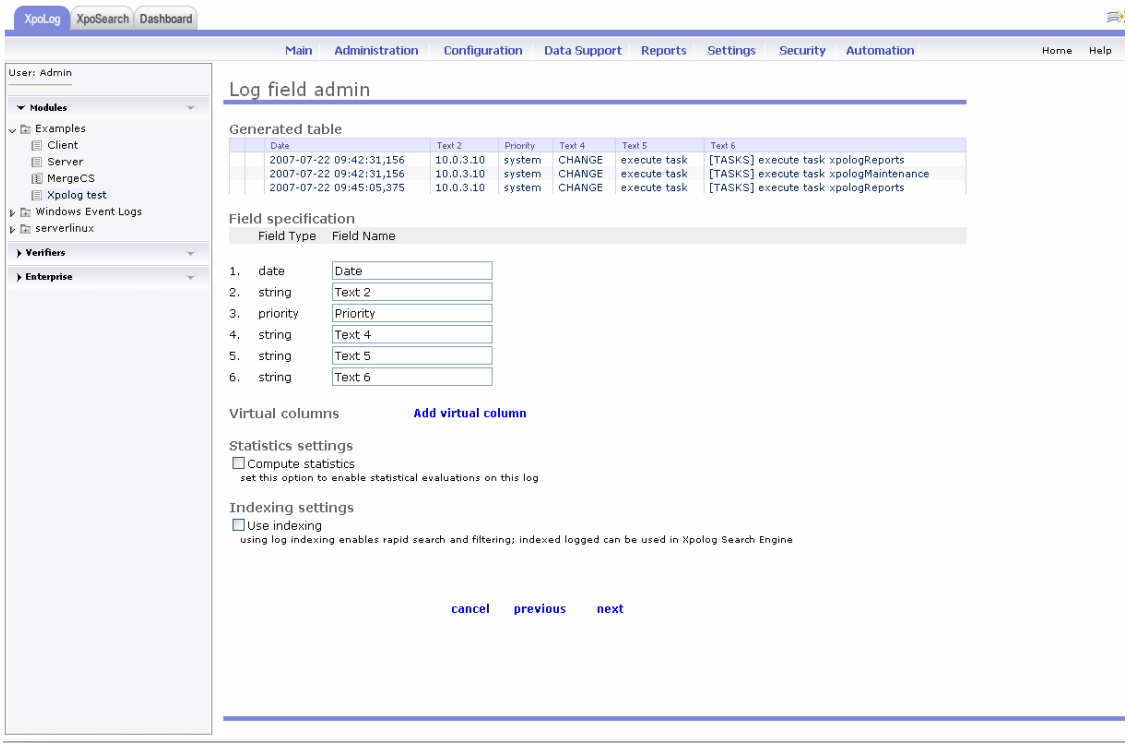
When done adding the desired pattern, click ‘Verify pattern’ to make sure that it was added correctly. The ‘pattern verification status’ will indicate whether the pattern is legal or not.



The ‘Log records analysis result’ will display a few lines from the parsed log.

Log view settings – Check the ‘Ignore unparsed records’ if you do not want XpoLog to show you records that does not match the log’s pattern. Check the ‘Show line number’ in case you want to see the log’s line numbers (NOTE: This option will slow down XpoLog a bit).

Click next in order to move on to the last screen of the log’s wizard

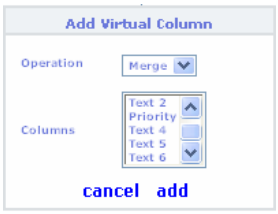


The third screen of the add log wizard

In this screen you can set the columns name, add a virtual column and set the statistics/indexing settings.

Rename columns – in the field name, enter the desired column name.

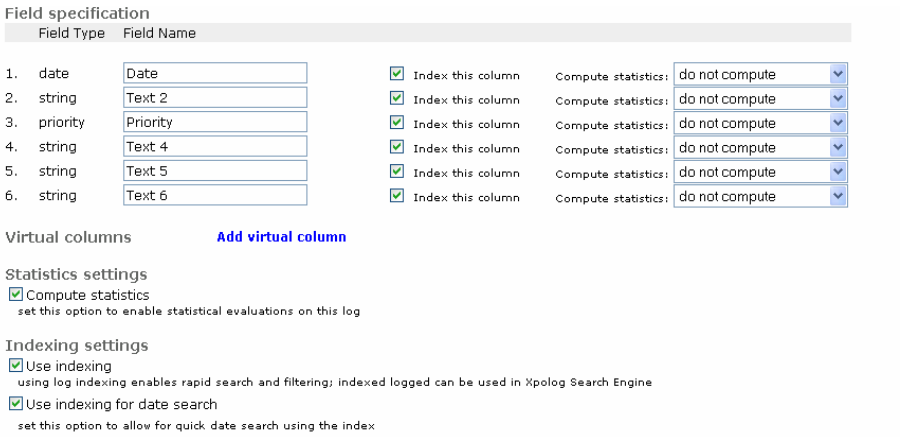
Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.



The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.

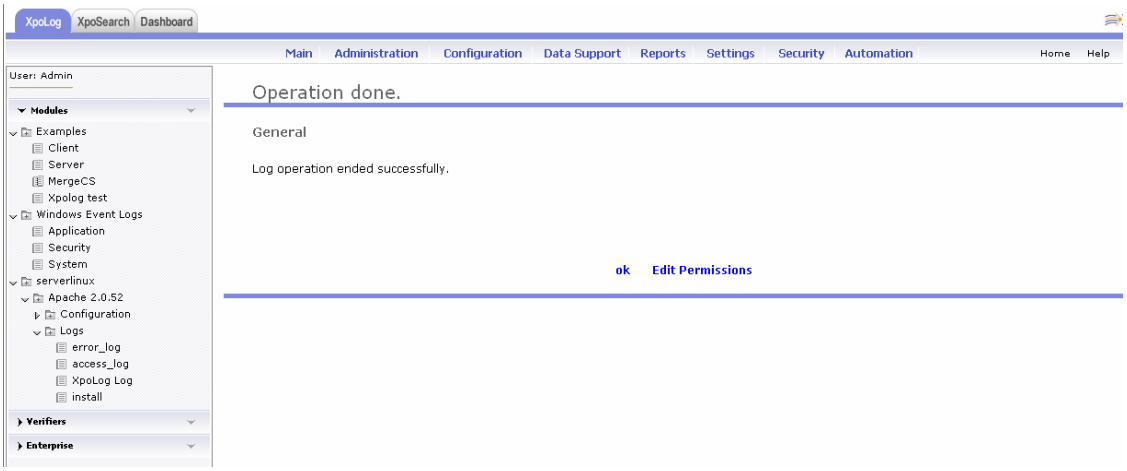
Indexing setting: check the ‘Use indexing’ in order to index the log. When the ‘use indexing’ is marked, a second indexing option appears: ‘Use indexing for date search’. For further information, please refer to XpoSearch.



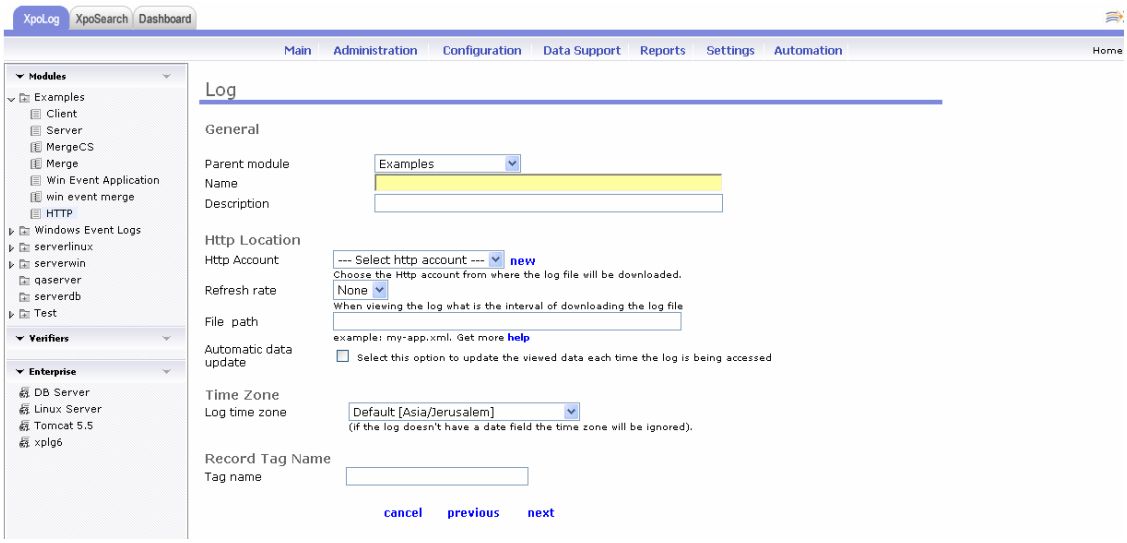
Statistical computation and indexing settings can be applied to each column separately

When done configuring the indexing, click ‘Next’.

The log’s wizard is done; Click OK to end the wizard. In case security is activated, you may edit the log’s permissions by clicking ‘Edit Permissions’.


XpoLog
XpoSearch
Dashboard
Main
Administration
Configuration
Data Support
Reports
Settings
Security
Automation
Home
Help
User: Admin
Modules
Examples
Client
Server
MergeCS
Xpolog test
Windows Event Logs
Application
Security
System
serverlinux
Apache 2.0.52
Configuration
Logs
error_log
access_log
XpoLog Log
install
Verifiers
Enterprise
Operation done.
General
Log operation ended successfully.
ok
Edit Permissions

10. Add HTTP XML log configuration:



You can create an HTTP XML log in XpoLog. From the data source administration, select ‘Add HTTP XML log configuration’.

Select the parent module for this log, and specify name and description.

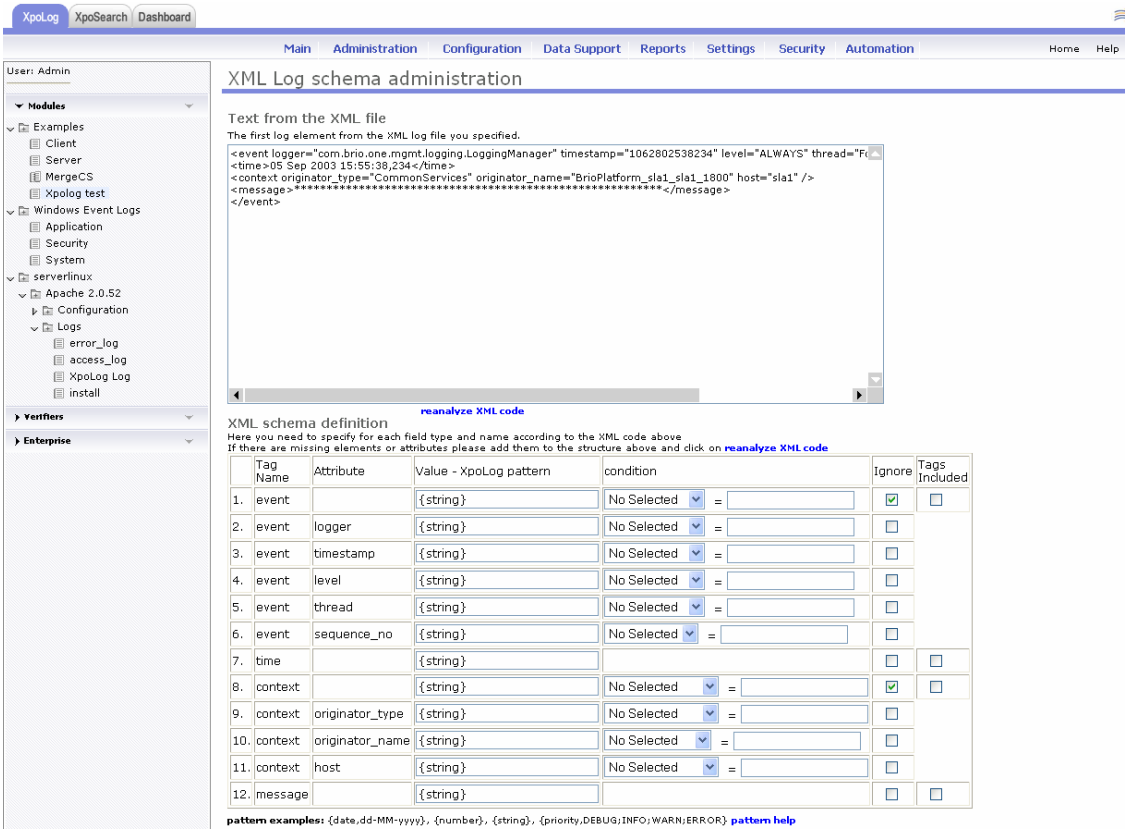
Select the relevant HTTP account for this log from the list of available accounts, or create a new HTTP account by clicking ‘new’. For further information on HTTP accounts, please refer to Data Support → Address book → HTTP.

Select the refresh rate in minutes for XpoLog to download the log file.

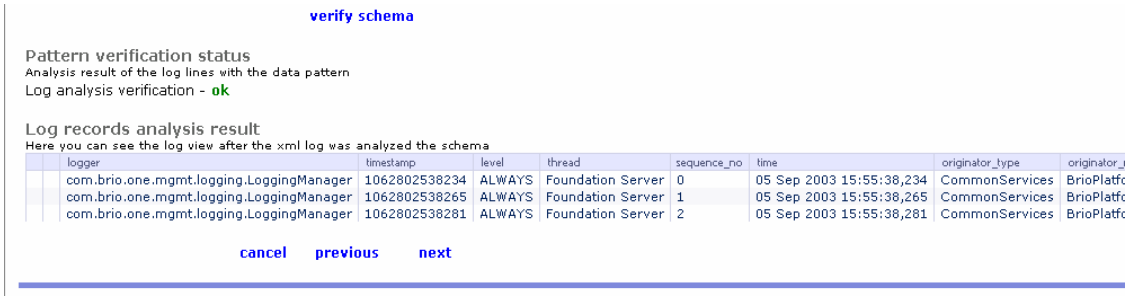
In the ‘file path’, you should supply the log’s relative path in the web site.

Selecting ‘Automatic data update’ will automatically update the existing data every time the log is accessed. Specify the log’s tag name, set the log’s time zone, and click ‘next’ in order to continue the log’s configuration.

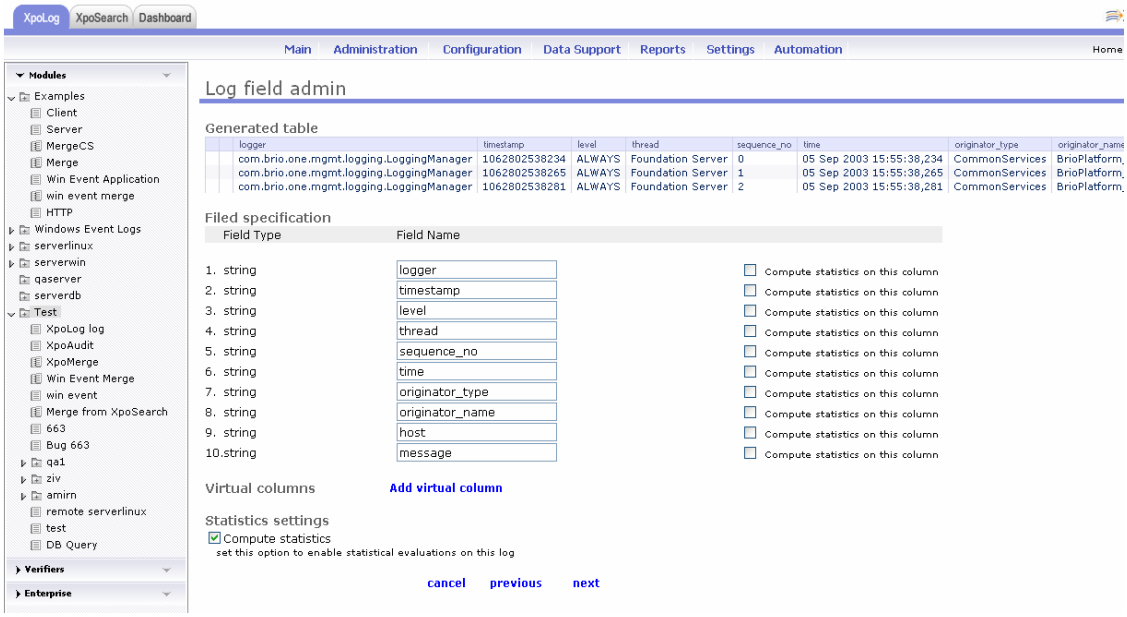
In the second wizard’s screen you will need to configure the XML log schema by specifying for each field type and name a pattern and a condition according to the XML code above. If there are missing elements or attributes please add them to the structure above and click the ‘Reanalyze XML code’.



Use the ‘Verify Schema’ to see a preview of the analyzed log according to the given pattern.

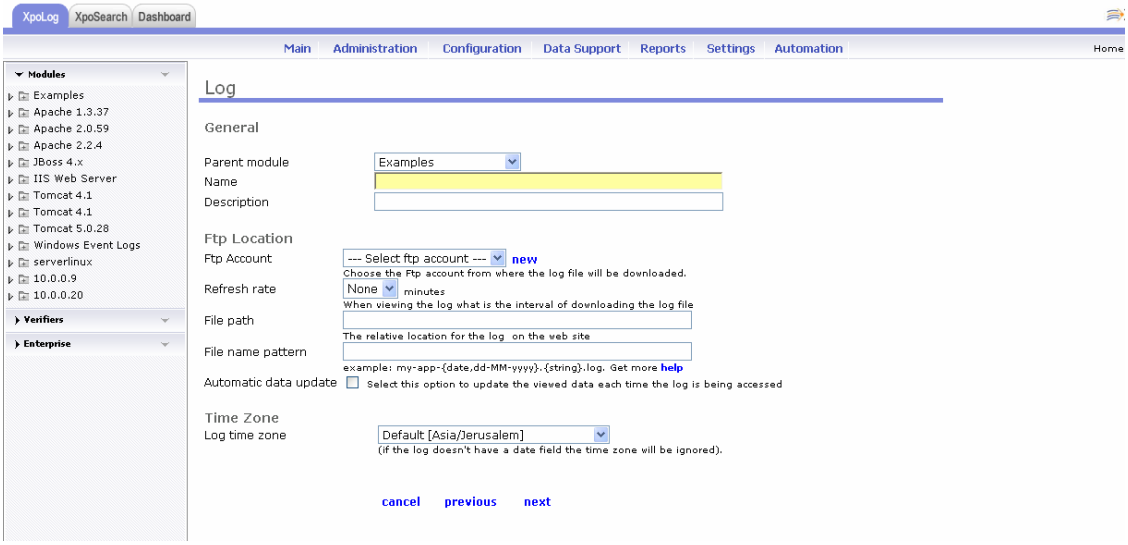


Click ‘next’ to move on to the last wizard’s screen, where you will have to configure the field specification, virtual columns and statistics computation.



Click ‘next’ in order to finish the log’s wizard. You may also go back, using the ‘previous’ link, and reconfigure the log’s properties.

11. <u>Add FTP log configuration:</u>



In order to create an FTP log in XpoLog, from the data source administration, select ‘Add FTP log configuration’.

Select the parent module for this log, and specify name and description.

Select the relevant FTP account for this log from the list of available accounts, or create a new FTP account by clicking ‘new’. For further

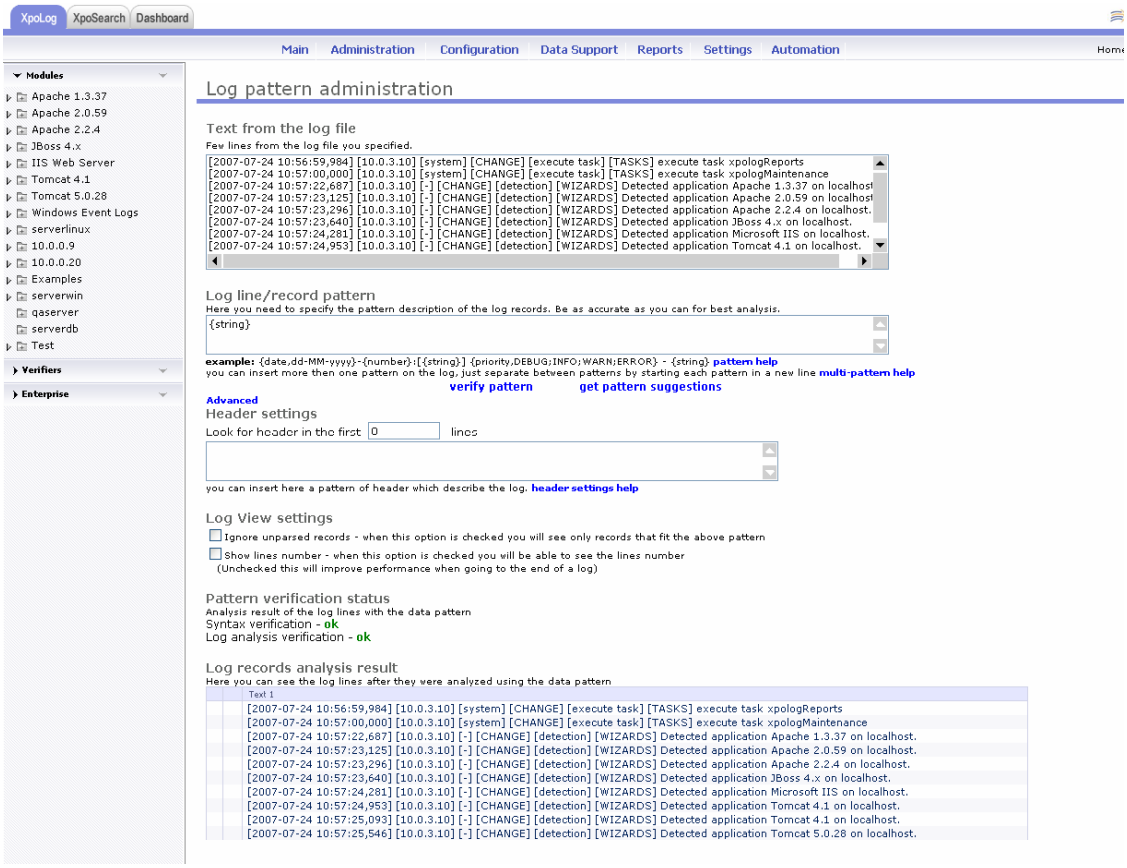
information on FTP accounts, please refer to Data Support → Address book → FTP.

Select the refresh rate in minutes for XpoLog to download the log file.

In the 'file path', you should supply the log's relative path in the web site.

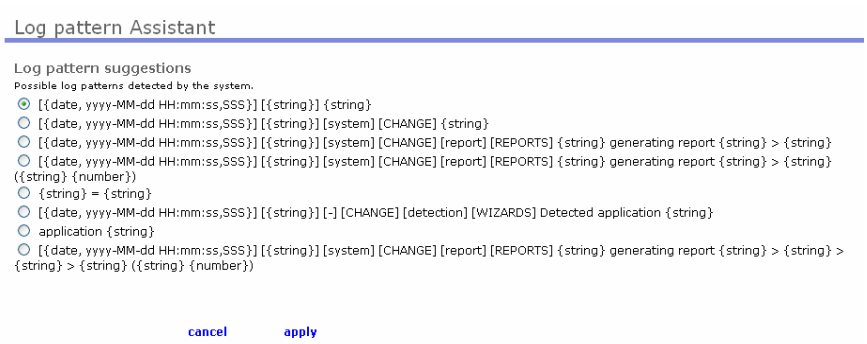
Selecting 'Automatic data update' will automatically update the existing data every time the log is accessed.

Select the log's time zone, and click 'next' in order to continue the log's configuration.



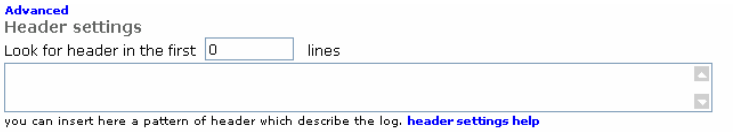
The 'Text from the log file' is a short preview of the log specified.

In the log line/record pattern specify a pattern according to the way you would like XpoLog to analyze the log. Click on the 'get pattern suggestions' and a few basic pattern alternatives to choose from, will be displayed.

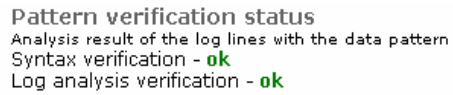


Header settings – set the number of lines according the log's header length in case you wish XpoLog to disregard the log's header.

You may add a separate pattern for the header as well.



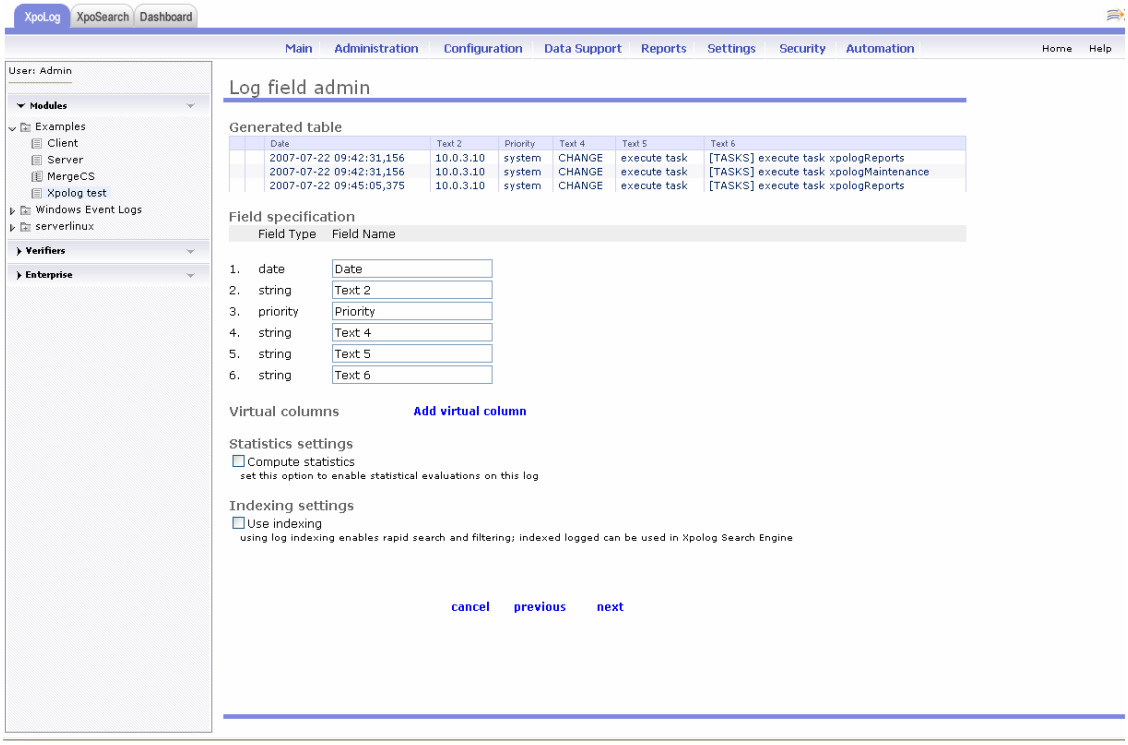
When done adding the desired pattern, click 'Verify pattern' to make sure that it was added correctly. The 'pattern verification status' will indicate whether the pattern is legal or not.



The 'Log records analysis result' will display a few lines from the parsed log.

Log view settings – Check the 'Ignore unparsed records' if you do not want XpoLog to show you records that does not match the log's pattern. Check the 'Show line number' in case you want to see the log's line numbers (NOTE: This option will slow down XpoLog a bit).

Click next in order to move on to the last screen of the log's wizard

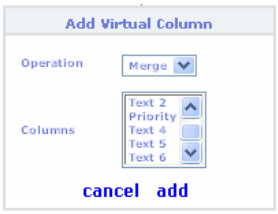


The third screen of the add log wizard

In this screen you can set the columns name, add a virtual column and set the statistics/indexing settings.

Rename columns – in the field name, enter the desired column name.

Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.

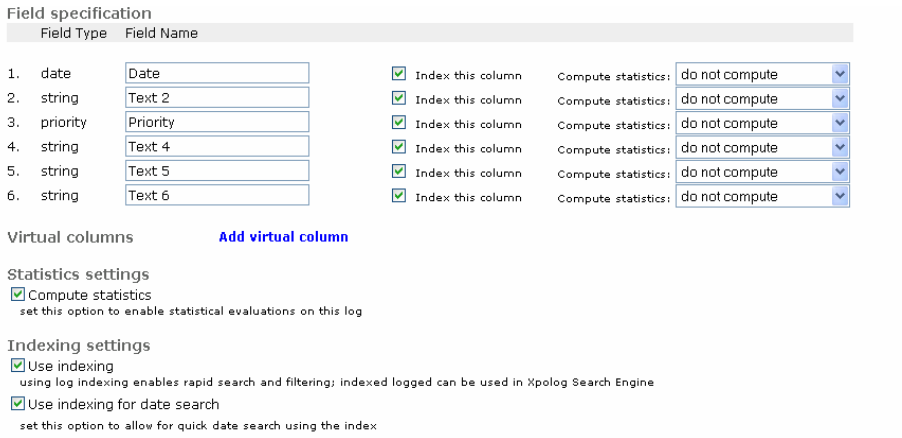


The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.

Indexing setting: check the ‘Use indexing’ in order to index the log. When the ‘use indexing’ is marked, a second indexing option appears:

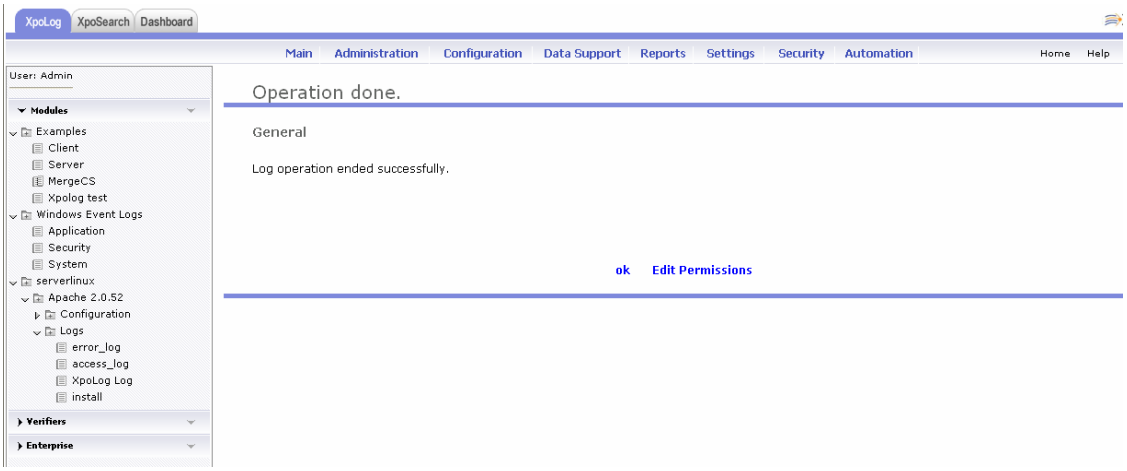
‘Use indexing for date search’. For further information, please refer to XpoSearch.



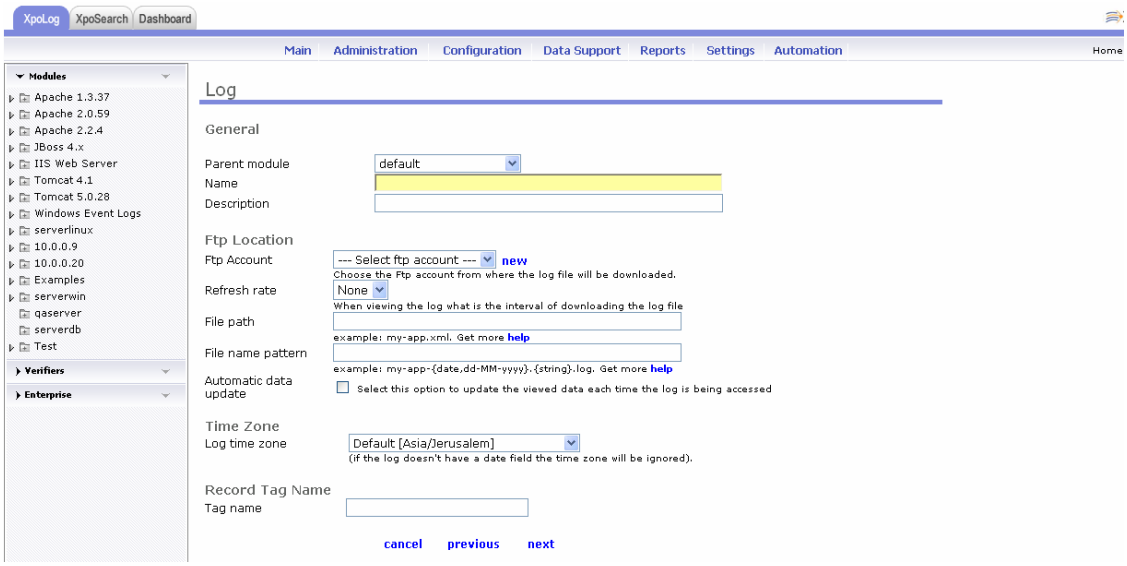
Statistical computation and indexing settings can be applied to each column separately

When done configuring the indexing, click ‘Next’.

The log’s wizard is done; Click OK to end the wizard. In case security is activated, you may edit the log’s permissions by clicking ‘Edit Permissions’.



12. Add FTP XML log configuration:



You can create an FTP XML log in XpoLog. From the data source administration, select ‘Add FTP XML log configuration’.

Select the parent module for this log, and specify name and description.

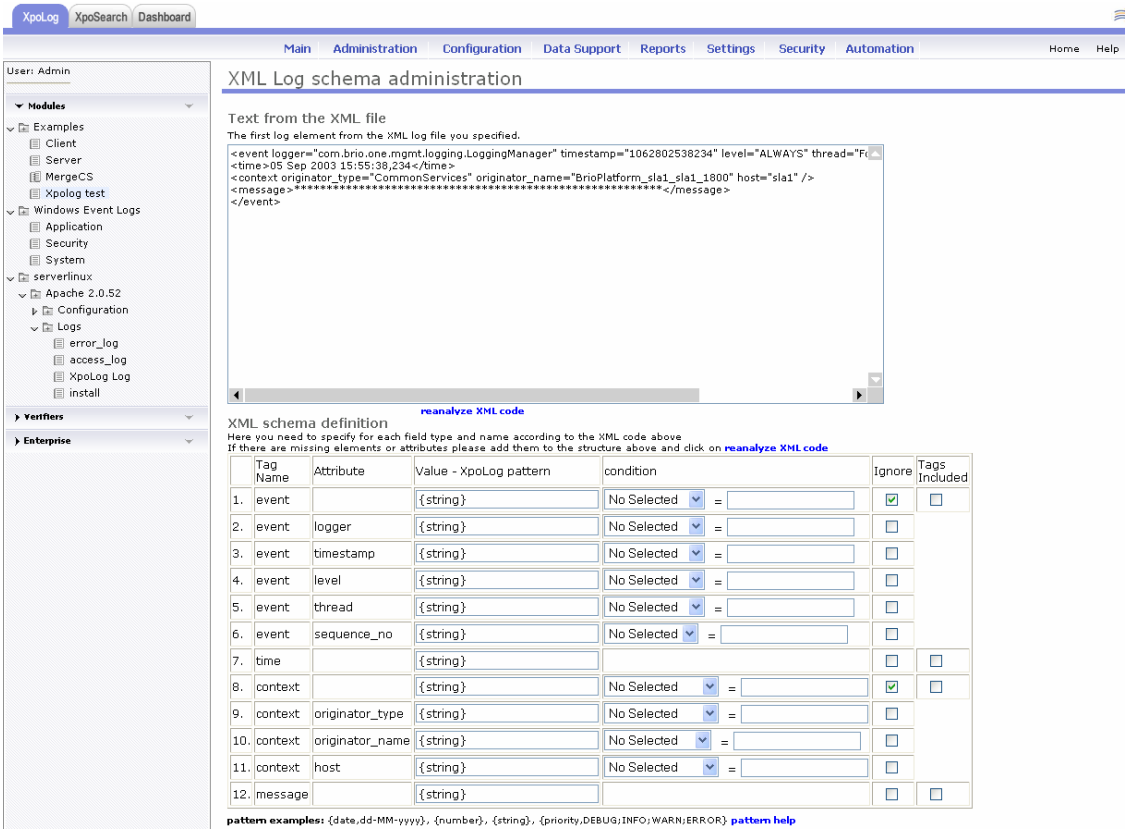
Select the relevant FTP account for this log from the list of available accounts, or create a new FTP account by clicking ‘new’. For further information on FTP accounts, please refer to Data Support → Address book → FTP.

Select the refresh rate in minutes for XpoLog to download the log file.

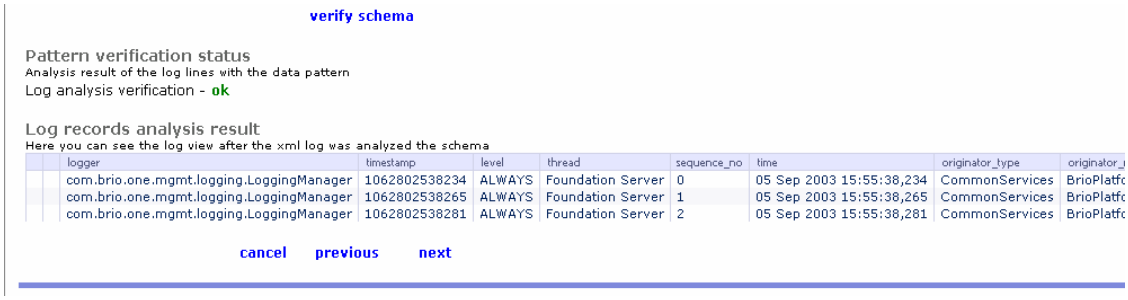
In the ‘file path’, you should supply the log’s relative path in the web site.

Selecting ‘Automatic data update’ will automatically update the existing data every time the log is accessed. Specify the log’s tag name, set the log’s time zone, and click ‘next’ in order to continue the log’s configuration.

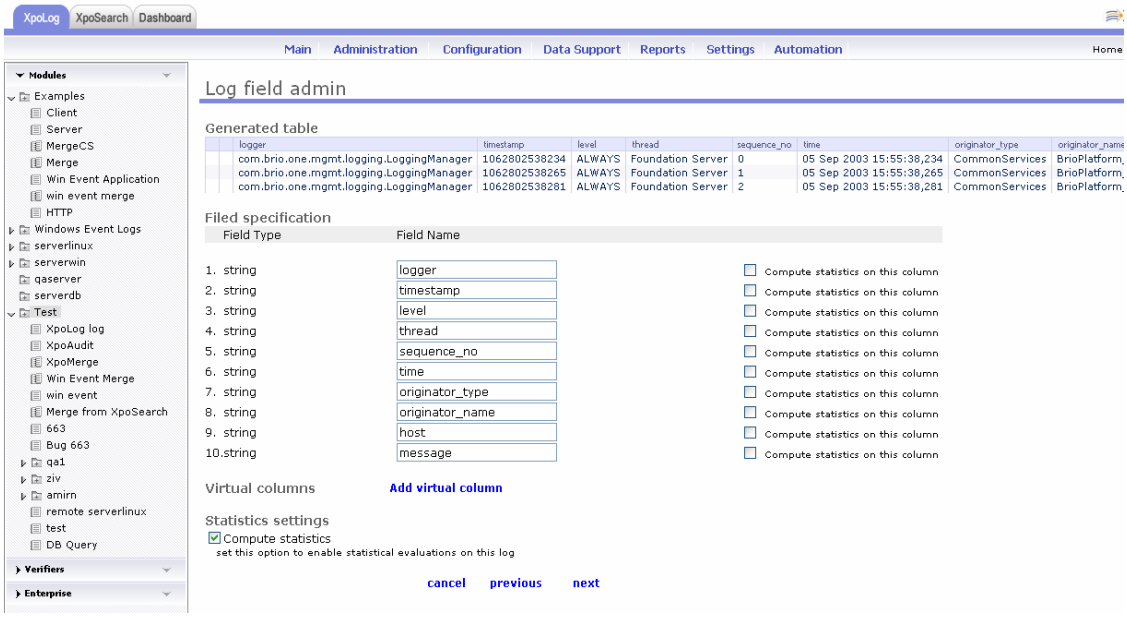
In the second wizard’s screen you will need to configure the XML log schema by specifying for each field type and name a pattern and a condition according to the XML code above. If there are missing elements or attributes please add them to the structure above and click the ‘Reanalyze XML code’.



Use the ‘Verify Schema’ to see a preview of the analyzed log according to the given pattern.

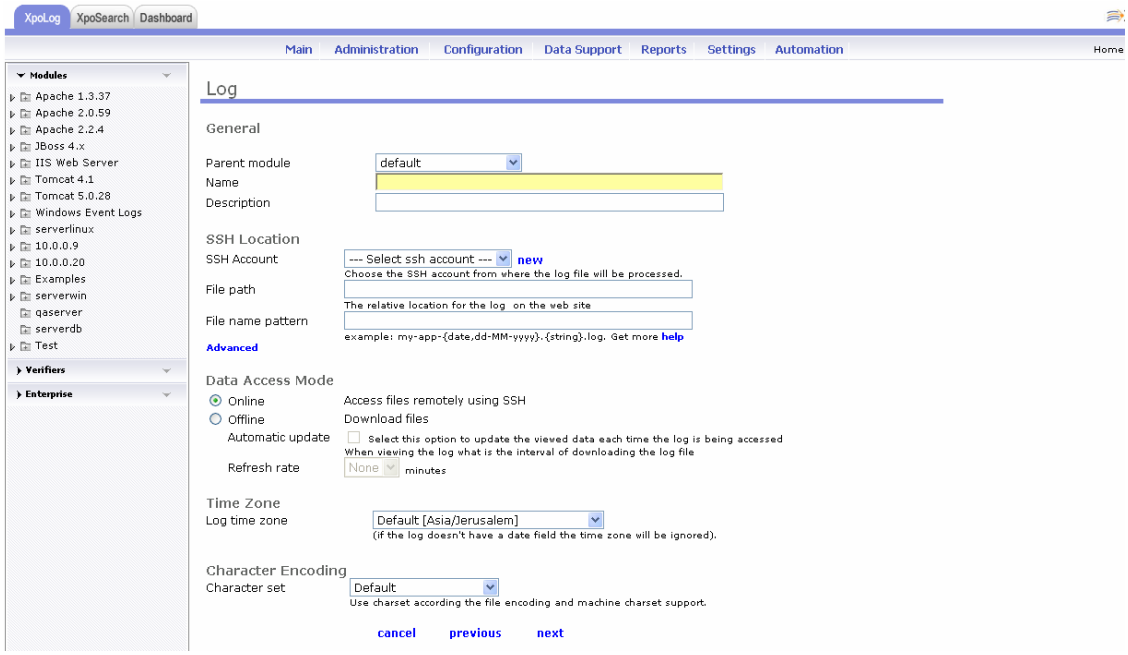


Click ‘next’ to move on to the last wizard’s screen, where you will have to configure the field specification, virtual columns and statistics computation.



Click ‘next’ in order to finish the log’s wizard. You may also go back, using the ‘previous’ link, and reconfigure the log’s properties.

13. <u>Add SSH log configuration:</u>



In order to create an SSH log in XpoLog, from the data source administration, select ‘Add SSH log configuration’.

Select the parent module for this log, and specify name and description.

Select the relevant SSH account for this log from the list of available

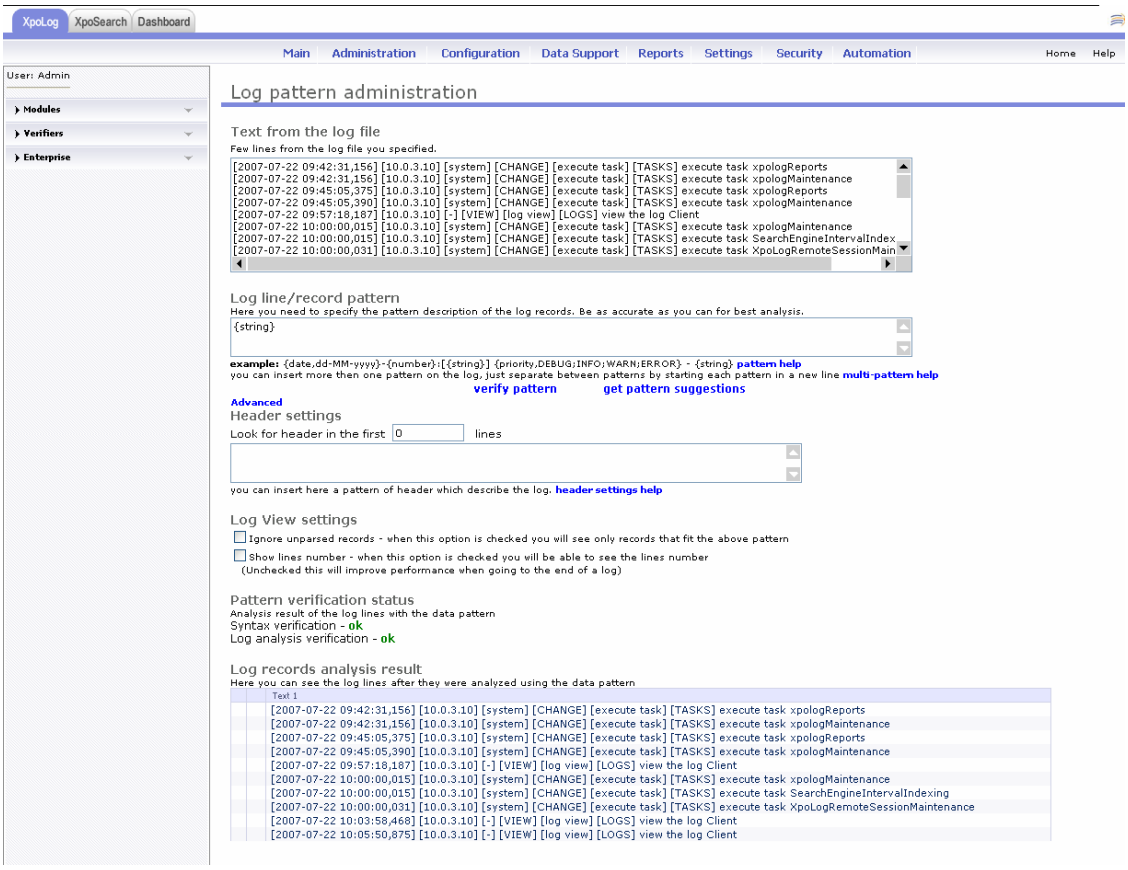
accounts, or create a new SSH account by clicking ‘new’. For further information on SSH accounts, please refer to Data Support → Address book → SSH.

Specify the log’s relative path in the ‘file path’, and the file name pattern for the log files.

Data access mode – The files can be accessed both online or offline. Select ‘online’ in order to access the files remotely, using SSH. Select ‘offline’ in order to download the log’s files. If the offline option was selected, you may set the automatic update option – in order to auto-update the data every time the log is accessed, or you may set a refresh rate in minutes instead.

Select the log’s time zone, and encoding. When done, click ‘next’ in order to continue to the wizard’s next screen.

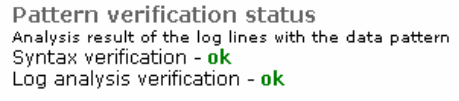
The next wizard screen is the log pattern administration:



The second screen of the add log wizard

A few lines from the log are presented in the ‘Text from the log file’ window. In the ‘Log line/Record pattern’ you need to add a pattern for the

selected log. When done adding the desired pattern, click ‘Verify pattern’ to make sure that it was added correctly. The ‘pattern verification status’ will indicate whether the pattern is legal or not.



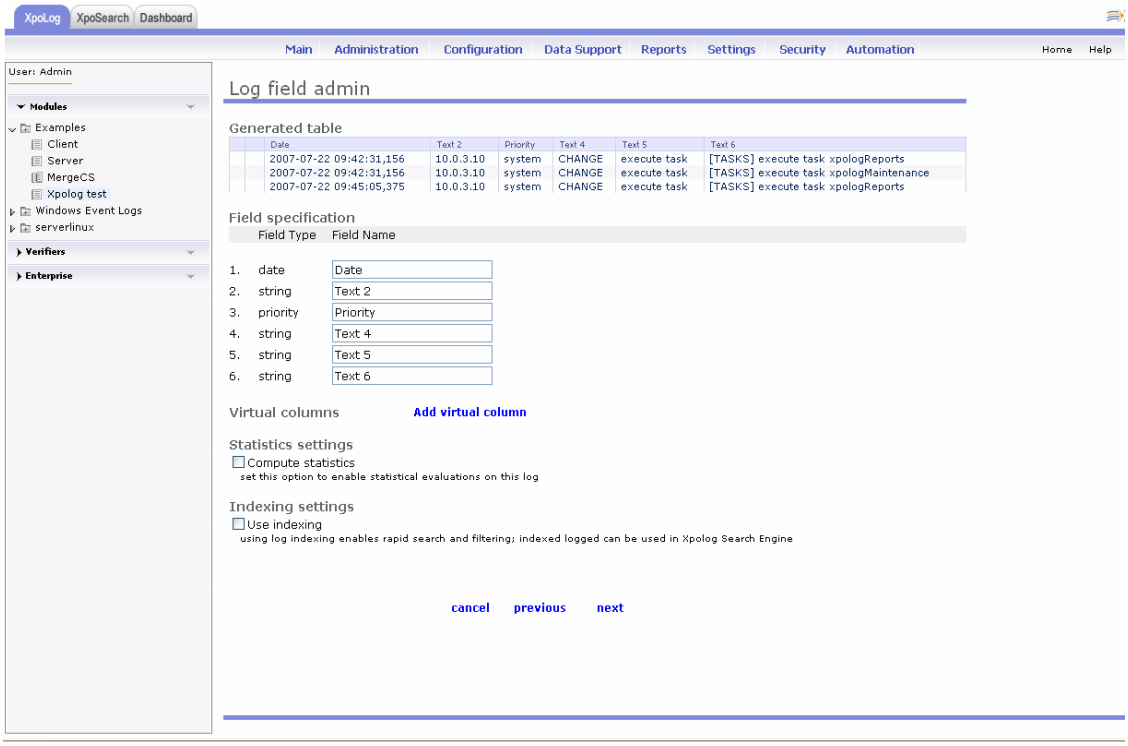
The ‘Log records analysis result’ will display a few lines from the parsed log.

Header settings – set the number of lines according the log’s header length in case you wish XpoLog to disregard the log’s header.

You may add a separate pattern for the header as well.

Log view settings – Check the ‘Ignore unparsed records’ if you do not want XpoLog to show you records that does not match the log’s pattern. Check the ‘Show line number’ in case you want to see the log’s line numbers (NOTE: This option will slow down XpoLog a bit).

Click next in order to move on to the last screen of the log’s wizard:

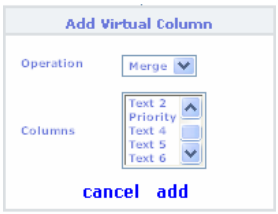


The third screen of the add log wizard

In this screen you can set the columns name, add a virtual column and set the statistics/indexing settings.

Rename columns – in the field name, enter the desired column name.

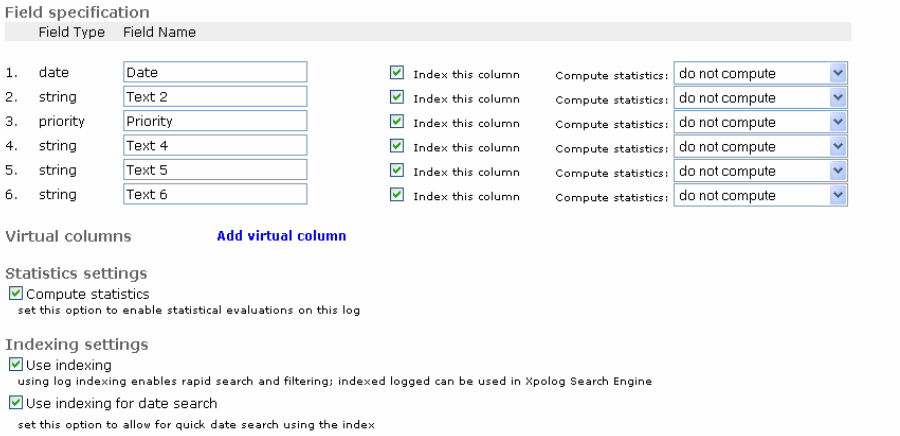
Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.



The add virtual column pop up window

Check ‘Compute statistics’ if you wish XpoLog to calculate statistics on the log. You may select statistics computation for each and every column separately. For further information, please refer to Dashboard.

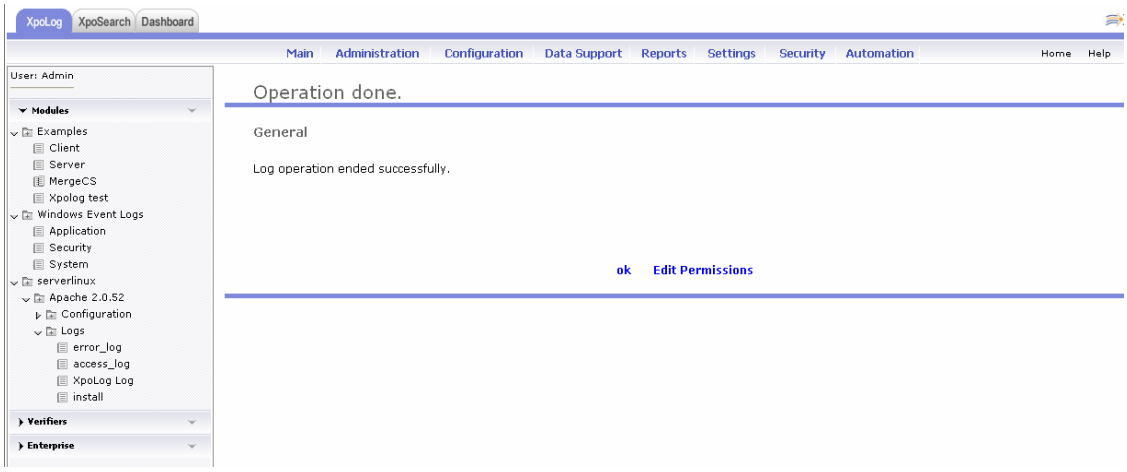
Indexing setting: check the ‘Use indexing’ in order to index the log. When the ‘use indexing’ is marked, a second indexing option appears: ‘Use indexing for date search’. For further information, please refer to XpoSearch.



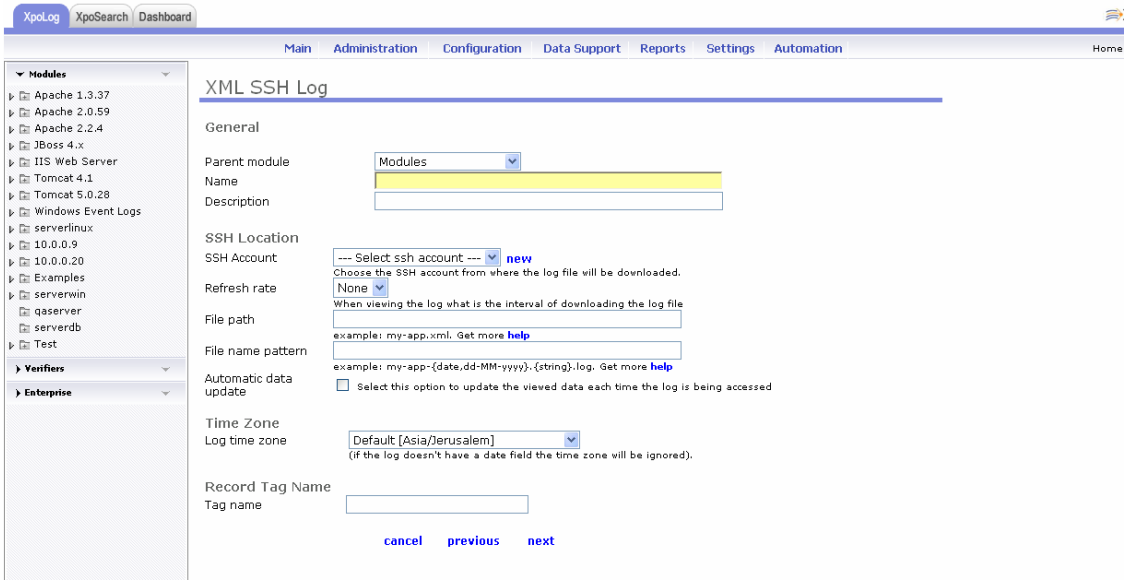
Statistical computation and indexing settings can be applied to each column separately

When done configuring the indexing, click ‘Next’.

The log’s wizard is done; Click OK to end the wizard. In case security is activated, you may edit the log’s permissions by clicking ‘Edit Permissions’.



14. <u>Add SSH XML log configuration:</u>



It is possible to create an SSH XML log in XpoLog. From the data source administration, select ‘Add SSH XML log configuration’.

Select the parent module for this log, and specify a name and description.

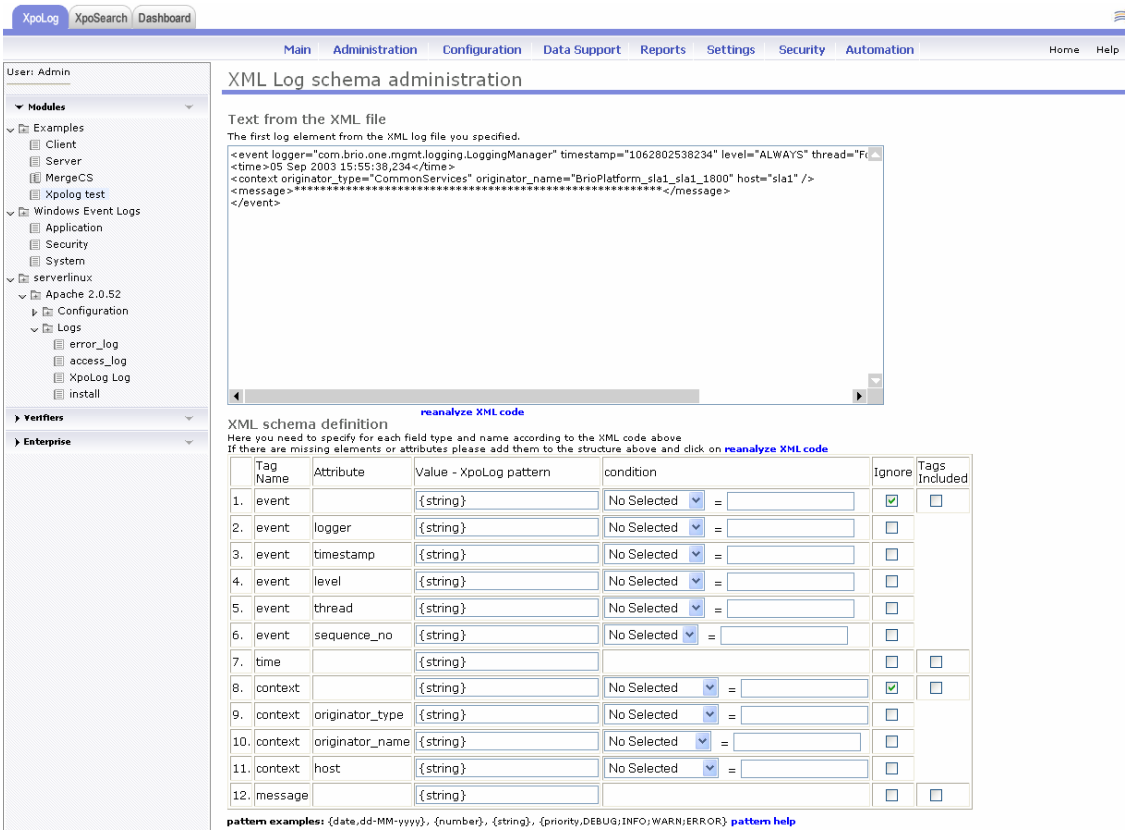
Select the relevant SSH account for this log from the list of available accounts, or create a new SSH account by clicking ‘new’. For further information on SSH accounts, please refer to Data Support → Address book → SSH.

Select the refresh rate in minutes for XpoLog to download the log file.

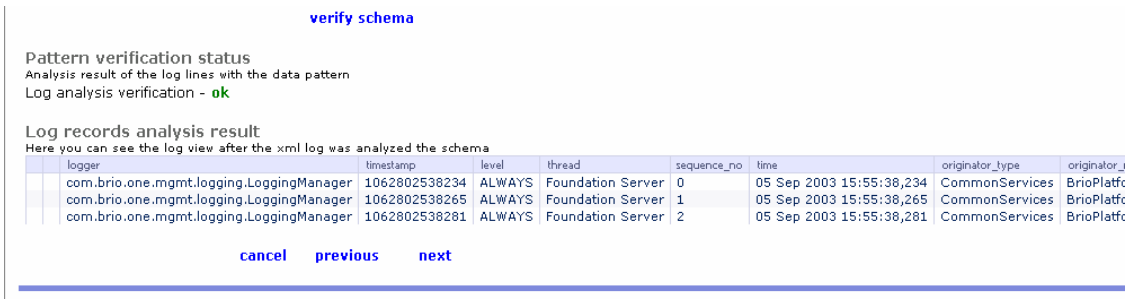
In the ‘file path’, you should supply the log’s relative path in the web site followed by its name pattern. Selecting ‘Automatic data update’ will

automatically update the existing data every time the log is accessed. Specify the log's tag name, set the log's time zone, and click 'next' in order to continue the log's configuration.

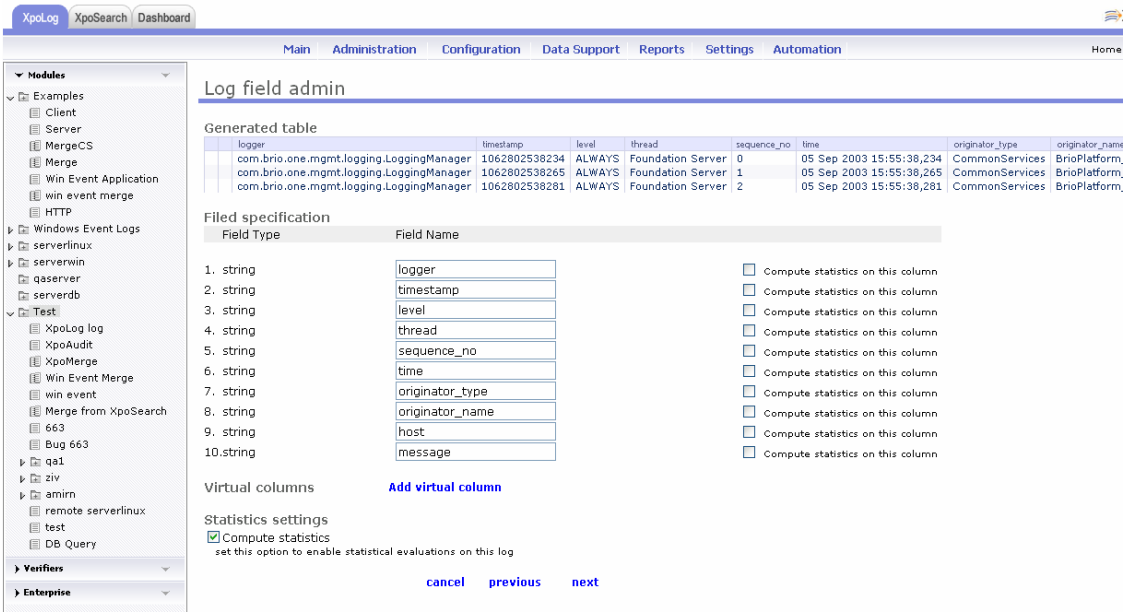
In the second wizard's screen you will need to configure the XML log schema by specifying for each field type and name a pattern and a condition according to the XML code above. If there are missing elements or attributes please add them to the structure above and click the 'Reanalyze XML code'.



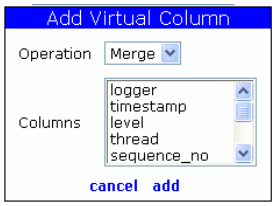
Use the 'Verify Schema' to see a preview of the analyzed log according to the given pattern.



Click ‘next’ to move on to the last wizard’s screen, where you will have to configure the field specification, virtual columns and statistics computation.



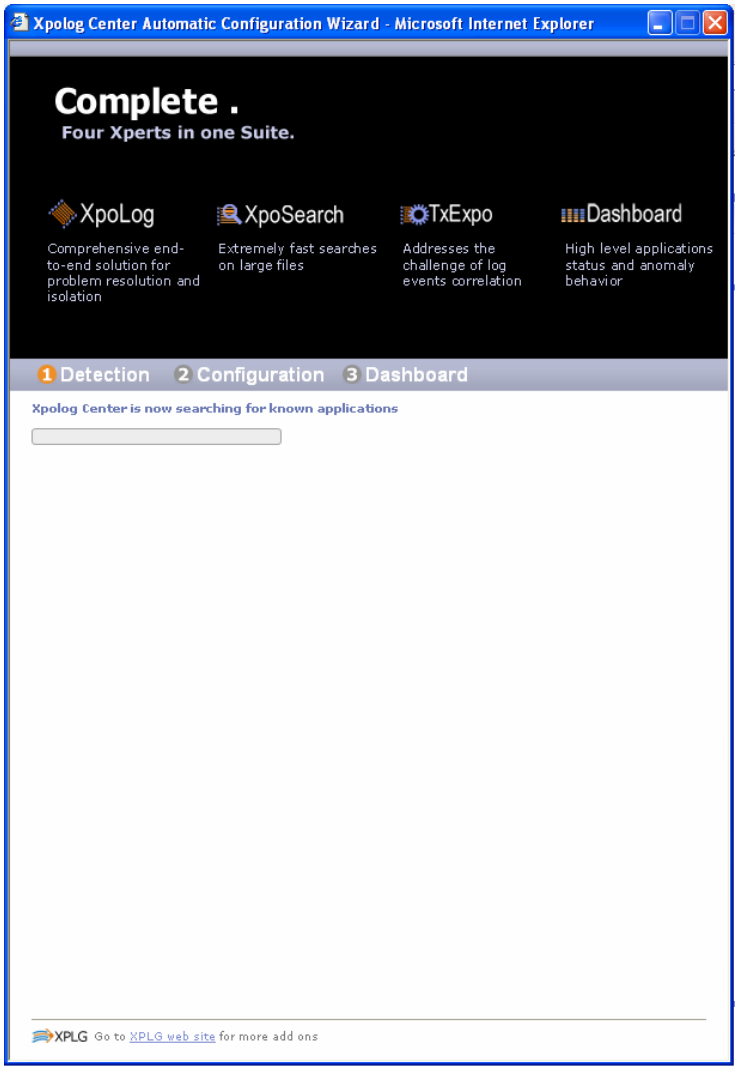
Add virtual column – click the ‘Add virtual column’, from the pop up window, select the desired column you wish to add and click ‘Add’.



The add virtual column pop up window

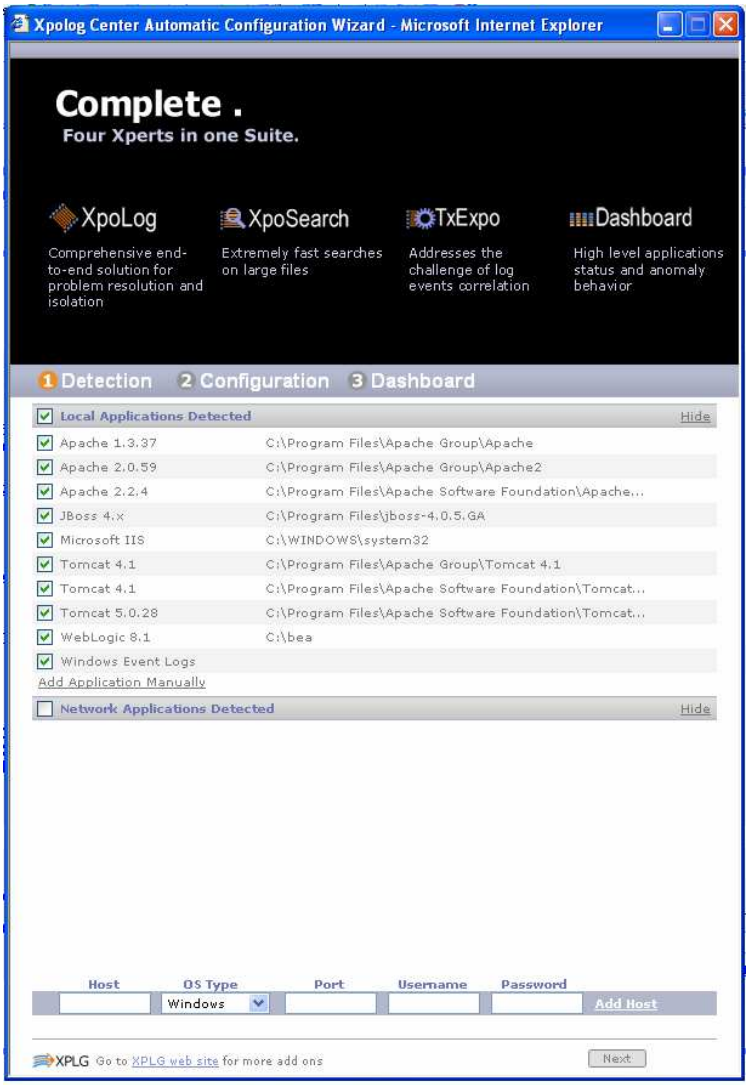
Click ‘next’ in order to finish the log’s wizard. You may also go back, using the ‘previous’ link, and reconfigure the log’s properties.

15. Automatic configuration wizard:



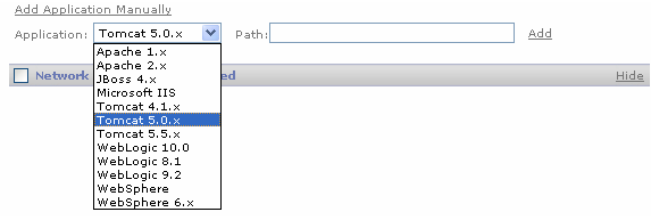
The automatic configuration wizard allows you to automatically detect and add logs from a list of known applications to XpoLog.

Click the 'Run automatic configuration wizard' in Administration → add log. In the first stage, the automatic detection processes will search for known application installed on your local machine, displaying available results.



At this stage, select all desired applications found on your local machine in order to add them to XpoLog.

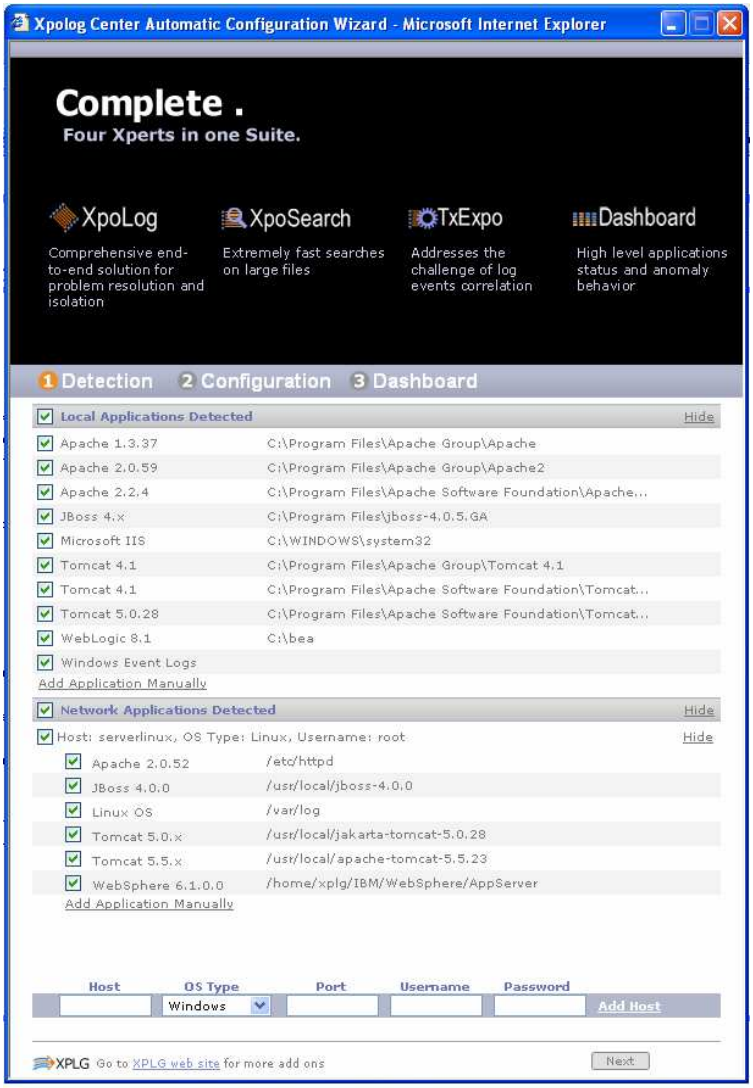
In case there is an application (On local machine) that the automatic wizard did not detect you may do so manually. Click the ‘add application manually’, select the application type from the list of available applications, specify it’s path, and click add.



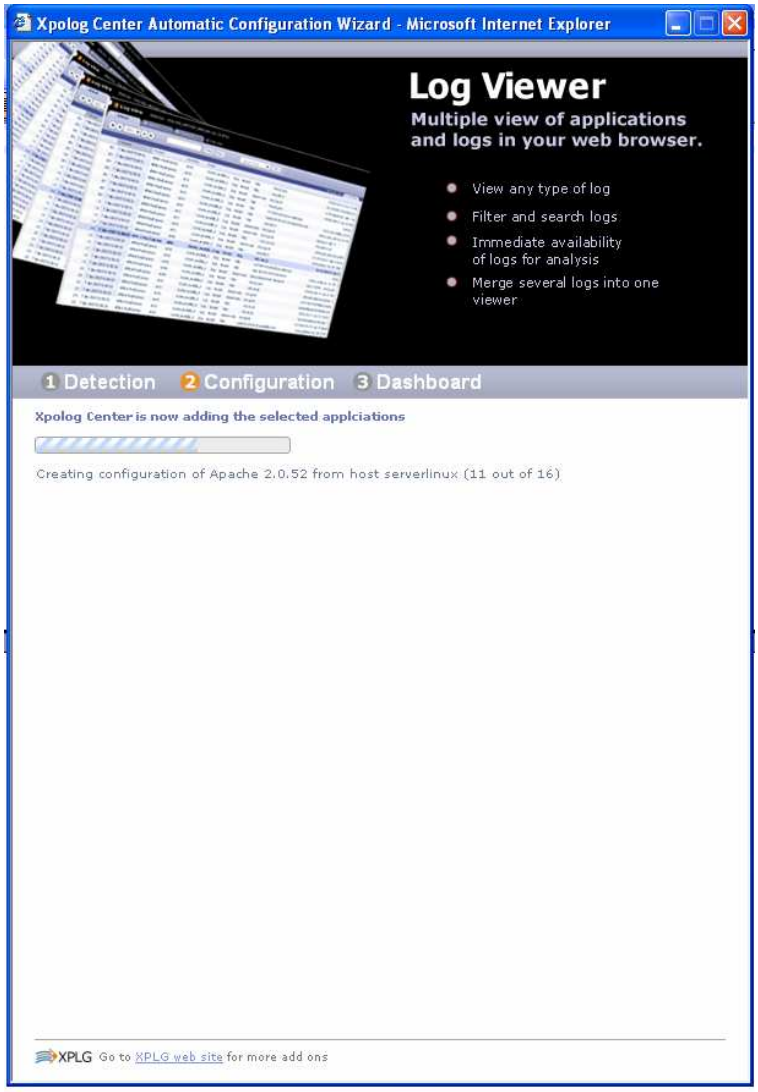
Network applications - The automatic detection wizard can add known applications' logs, located on remote machines in your network to XpoLog as well. Specify a host name for the machine that hosts the logs you wish to add, select the host's operating system, the connection port and a username and password. Click 'Add host'

The automatic detection wizard will search for known applications and add all available logs. You can add applications manually from the network, in a similar way as in local applications.

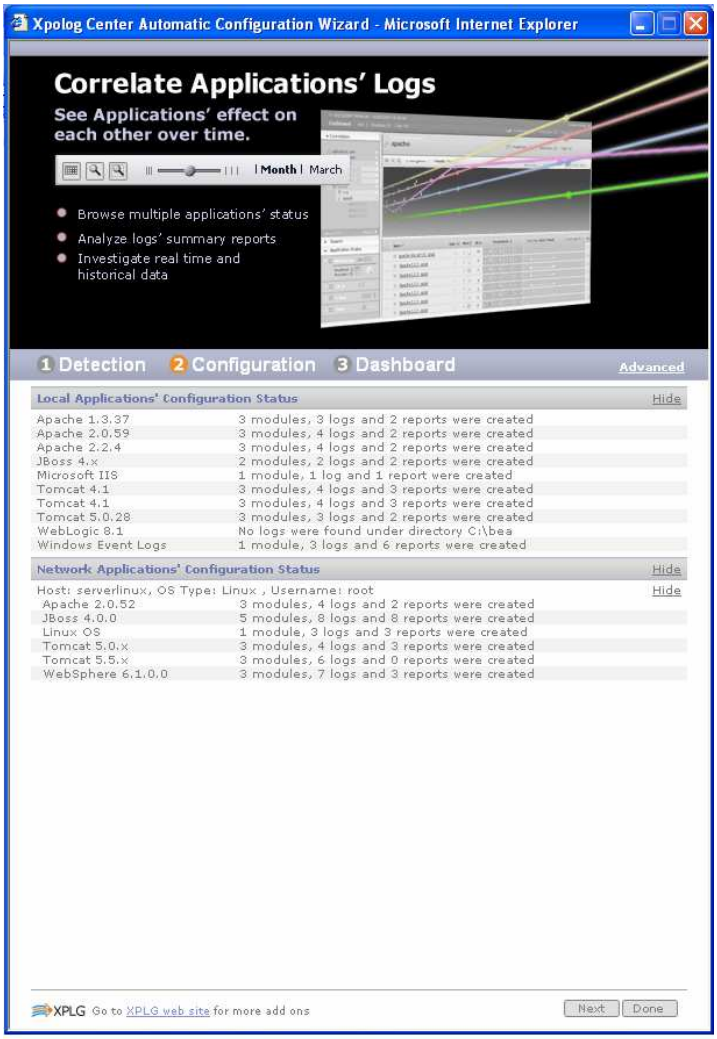
When finished adding all desired applications, click 'Next'



The automatic detection is now creating the configuration for all the selected applications.



When the configuration stage is finished, a list of all the modules, logs and reports created, both from local host and from the network is displayed.



At this point you can click ‘Done’, finish the automatic detection wizard and go back to XpoLog, or click ‘Next’, and the wizard will compute statistics and generate the reports created for the new logs added. The statistics computation and the report generation may be completed at a later time. For further information regarding statistics, please refer to Dashboard.

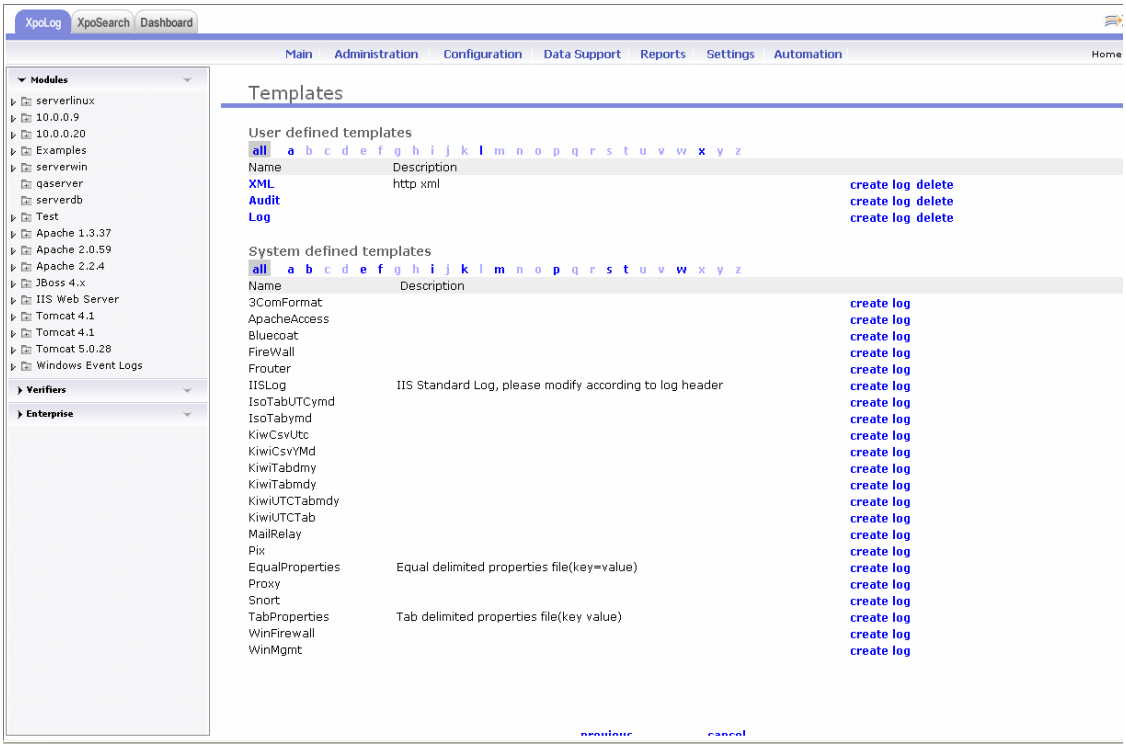
When the automatic detection process is done, you can either carry on configuring logs by clicking: ‘Configure more’ and you will be directed to the ‘data source administration’ in XpoLog’s main window.

Or, you may go to each on of the options listed on the right:

Dashboard, Log Viewer, Search Engine, Reports, Diagnostics.

If you don’t want XpoLog to start the automatic configuration wizard every time XpoLog starts, mark the check box in the lower left corner of the detection wizard.

16. Create from Template:



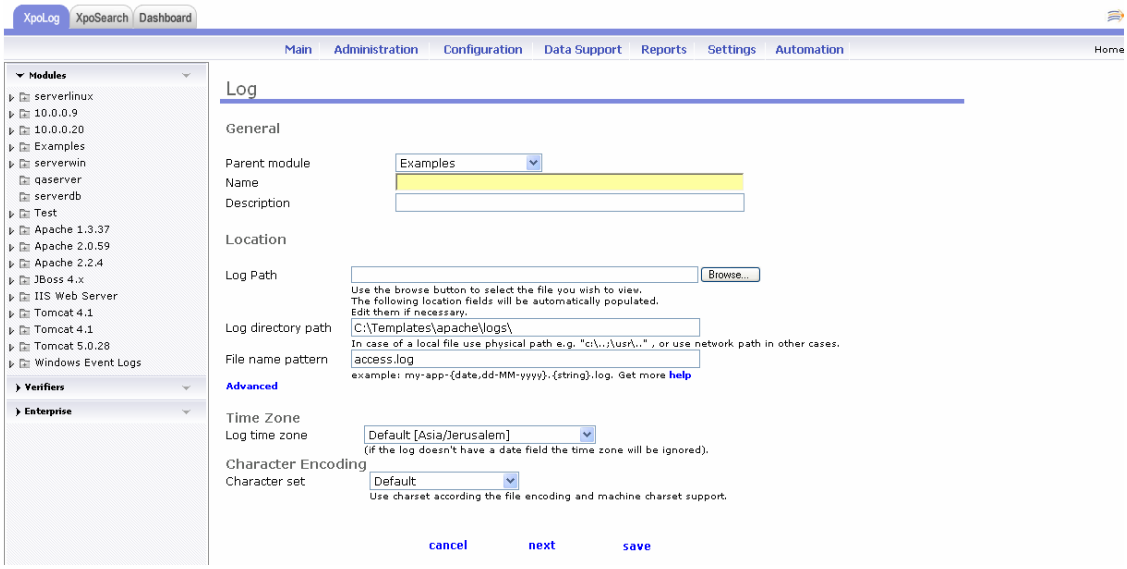
A log can be created using predefined templates.

There are two kinds of templates: User defined and system defined.

For further information regarding the user defined templates please refer to configuration → Save as template.

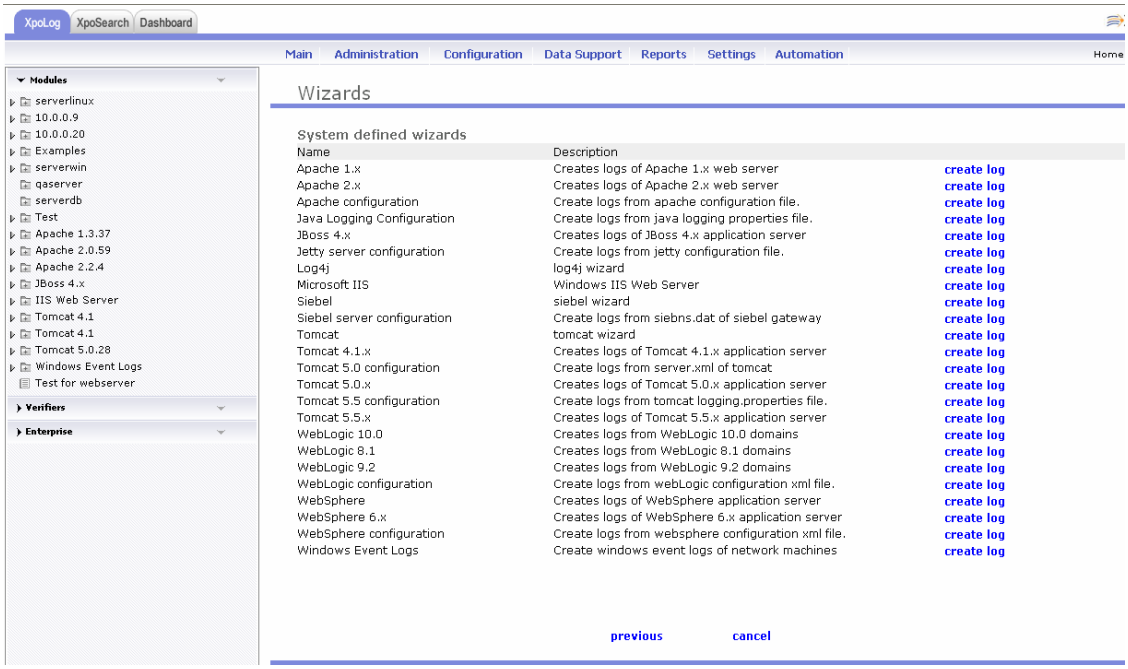
Click the ‘Create log’ link opposite the desired log template you wish to add, and start configuring the log.

For example, adding the Apache access log using the Apache Access template.



The following log's wizard and the steps that needs to be done in order to finish this wizard, is similar to the 'Add log manually' paragraph, described in the administration→add log chapter.

17. <u>Create from Wizard:</u>

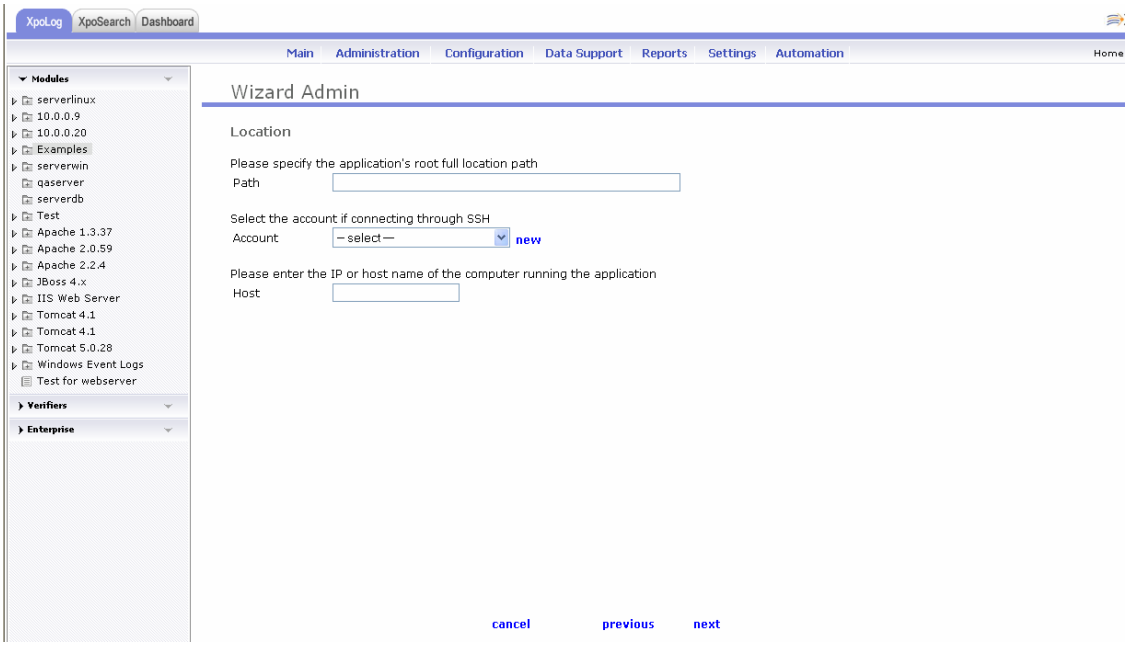


Creating a log using the system defined wizards helps you to add logs from a selected list of popular applications with minimum difficulty.

Select an application from the list, and click 'create log'.

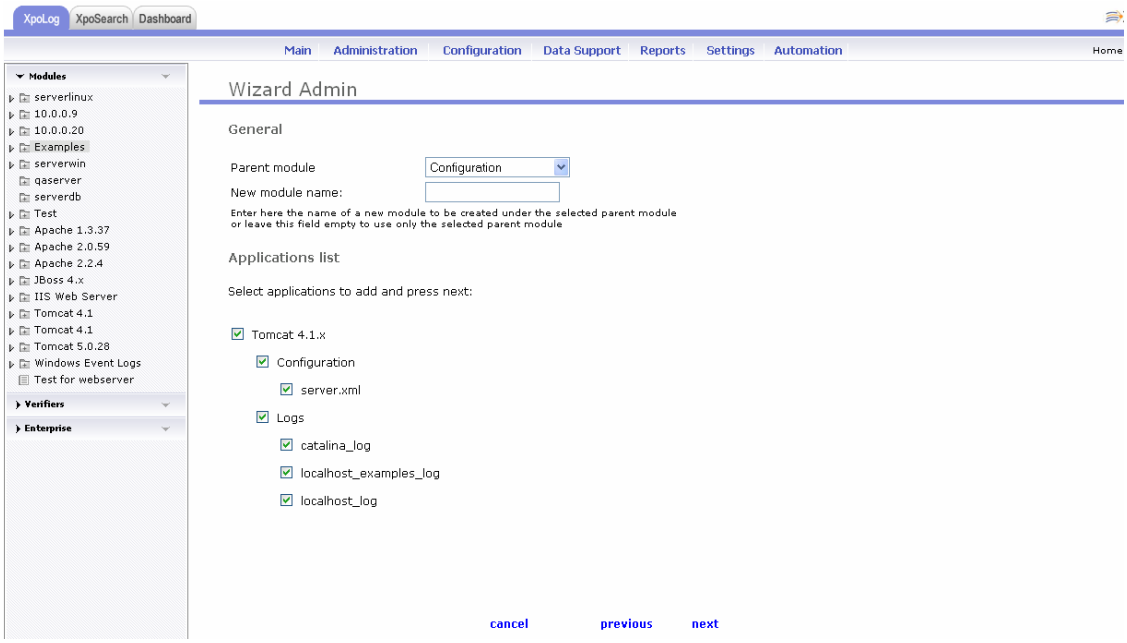
For example, creating a log for Tomcat 4.1.x:

Click the ‘create log’ link, opposite ‘Tomcat 4.1.x’



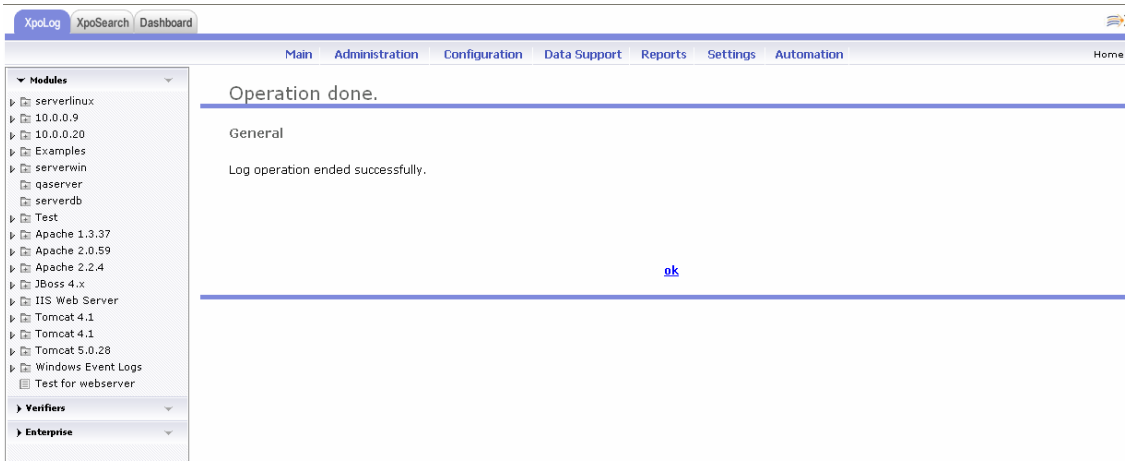
Please specify the log’s path, select an account if needed (If connecting thorough SSH) from the list of available accounts or create a new account, by clicking ‘new’ next to the accounts list. For further information regarding accounts, please refer to ‘Data support → address book → SSH.

Specify the host name, or leave empty if the logs are located locally.



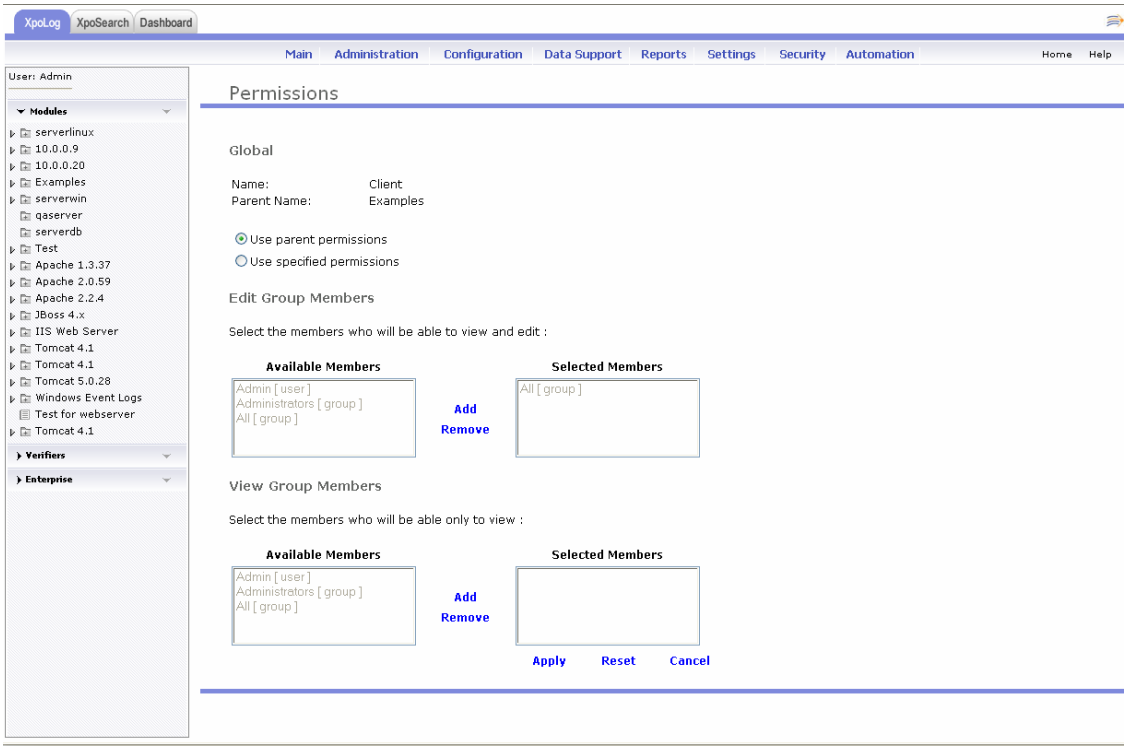
Select a parent module for the log, or enter a new module name in the empty field (I.e. ‘Tomcat 4.1’ located inside module ‘Configuration).

From the ‘Application list’, select all available logs for Tomcat 4.1.x. Click ‘Next’ and in the next screen, click ‘Ok’ to confirm the successful end of the wizard.



- **Edit log -** In order to edit an existing log via the administration menu, the specific log should be in focus. Select the relevant log in the left pane in the log viewer. When the log is in focus, open the administration menu and click ‘Edit log’. The log’s wizard (Similar to the add log wizard) is now available for you to make changes in it. Browse through the wizard using ‘next’ until completing it.
- **Edit log’s permissions** – Editing the log’s permissions enables you to set edit/view permissions for specific users/groups. Editing the log’s permissions is only available when security is activated. For further information on security, please refer to Settings → General.

  Select the relevant log in the left pane in the log viewer. When the log is in focus, open the administration menu and click ‘Edit log’s permissions’.



There are two options to set permissions:

1. ‘Parent permissions’ – this will set the same permissions as set in the parent module.
2. ‘Use specified permissions’ – selecting this option will allow you to add or remove users/groups from both available options: Edit group and the View group.

   Click ‘Reset’ in case you would like to discard all changes, or click ‘Apply’ in order to save changes.

- **Edit log's Meta data** – Meta data selection – you can select a Meta data from a list of predefined Meta data schemes. For further information regarding Meta data, please refer to Data support → Meta data.

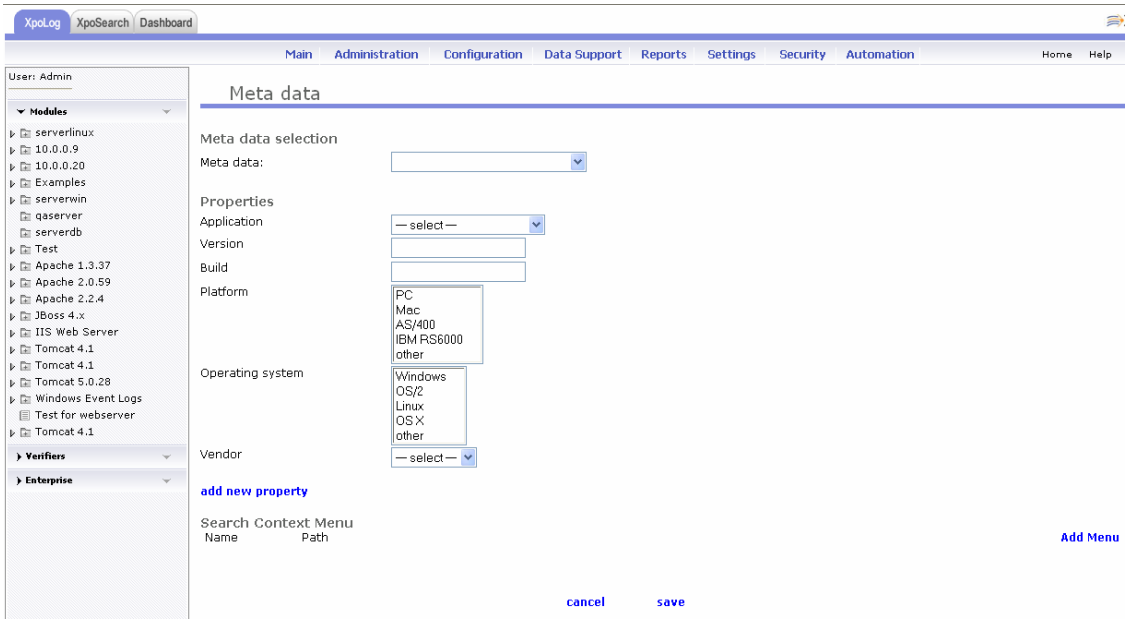
  Properties – Application: select the most suitable application for the specific log from the list of predefined applications.

  Specify the application version, build, platform, operating system and the vendor.

  Add new property – you can add new property to the metadata by clicking 'add new property' link. New section will appear, enter the property type and value in the textboxes.

  Add menu – you can add new search context by clicking 'Add menu' link. New section will appear, enter the search name in the 'Name' textbox and the search's source in the path textbox.

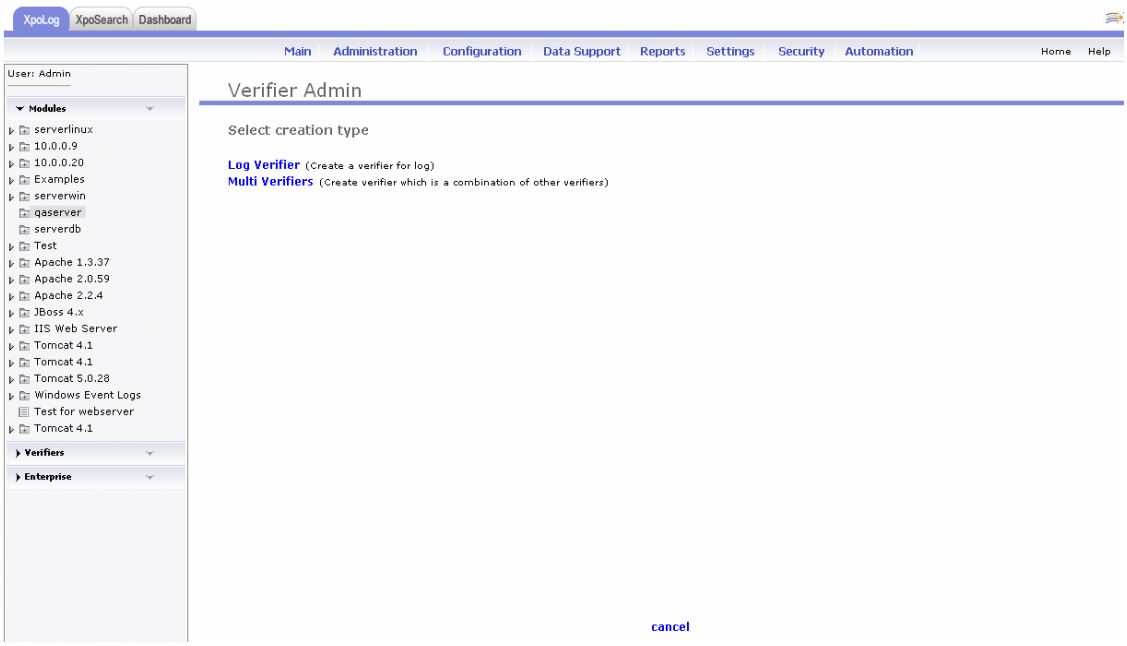
  You can use the this metadata by right clicking on the relevant log view, selecting 'Search' and choosing the desire search context name.



- **Remove log** – in order to remove a log, select the relevant log in the left pane in the log viewer, and when the log is in focus, open the administration menu and click ‘Remove log’. Clicking ‘Ok’ will confirm deletion of log. In case you don’t want to delete it, click ‘Cancel’.

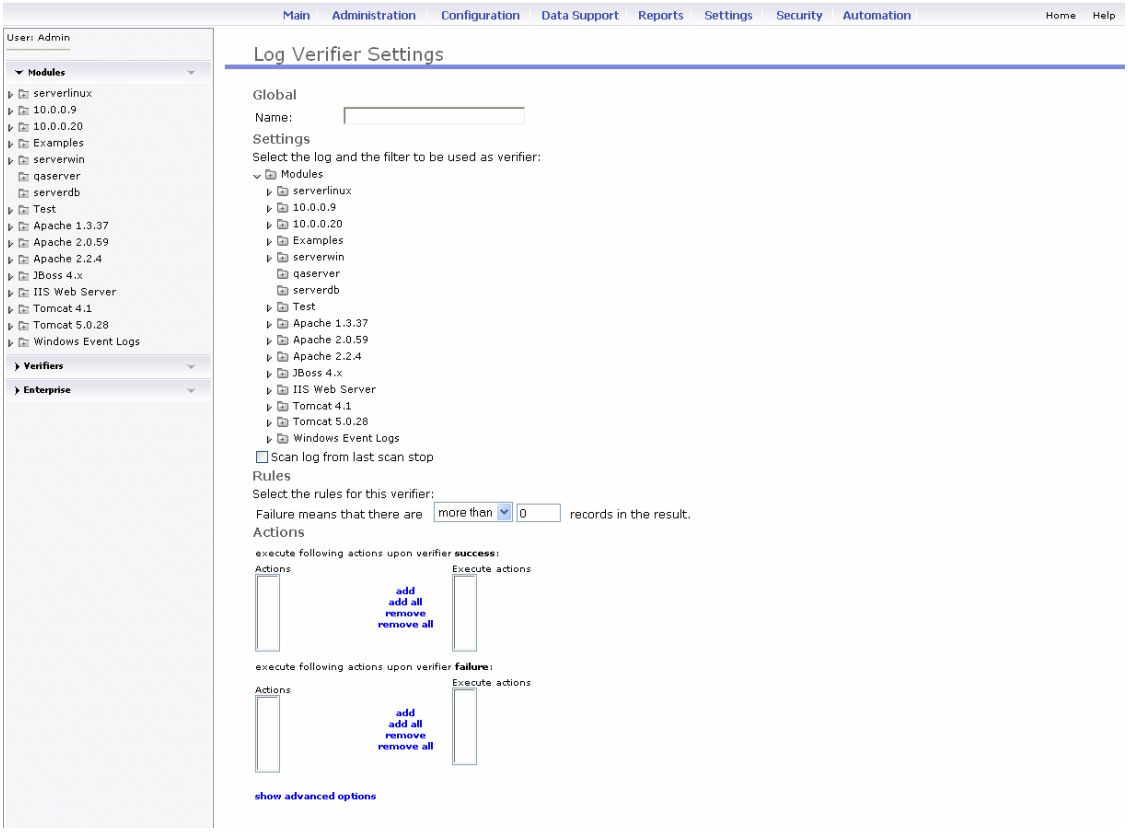
Verifier

Add verifier:

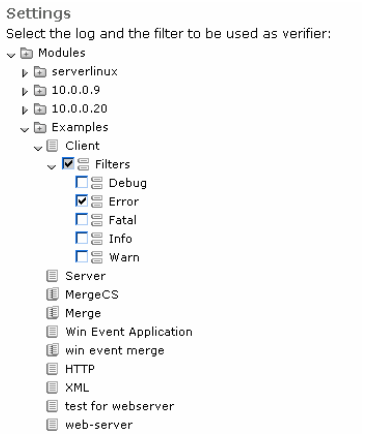


There are two different kinds of verifiers in XpoLog: Log verifier – works on a specific log, while Multi verifiers - is a combination of numerous log verifiers.

Log Verifier – A verifier is a mechanism that allows you to validate your system's health based on your logs and the filters defined for them. For instance, X number of 'ERROR' occurrences in the log may indicate that something is wrong. When you run a verifier (either manually or automatically) the verifier can execute different type of tasks according to the result. You can create multiple verifiers to examine the entire system state.



In the verifier's wizard, specify a name for the verifier. Drill down in XpoLog's tree to select the relevant log's filter.

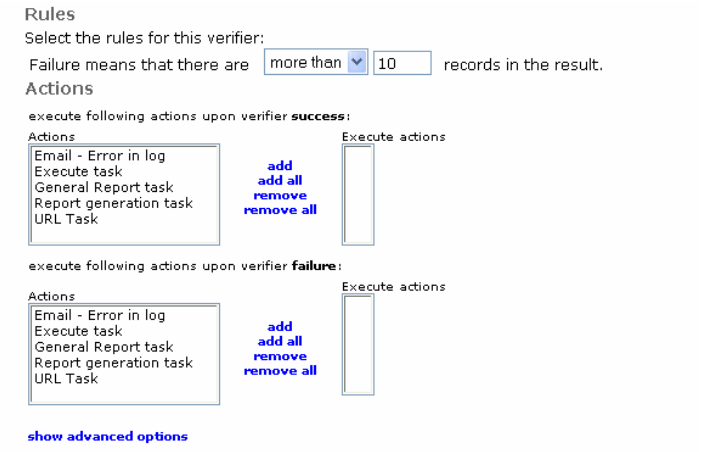


Check the 'Scan log from last scan stop' if you don't want XpoLog to scan the whole log every time you activate the Verifier.

Rules – you can set failure/success rules for the verifier by specifying the number of results along with a relevant condition.

Actions – you may want XpoLog to execute a few actions in case the verifier fails/succeed. Use the add/remove commands in order to set a list of actions for

the verifier. For further information regarding tasks (Actions), please refer to Automation → Tasks.

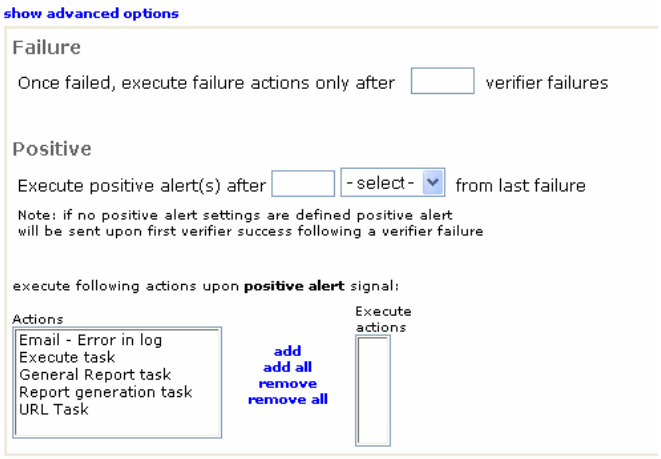


Advanced options – Failure – you can set XpoLog to execute a task upon verifier's failure only after X times it fails, instead of executing this task after each time the verifier fails.

Positive – you can set XpoLog to send a positive alert (A certain task) in 2 ways:

1. Set a time rule – Send a positive alert if the verifier doesn't fail in a certain time frame. I.e. – Send a positive alert 30 minutes after the last verifier's failure.
2. Send a positive alert after the next verifier's success. In that case, the time fields should be left empty.

The last thing you should configure is the task you would like XpoLog to execute as a positive alert.



Click 'Save' to finish the verifier wizard.

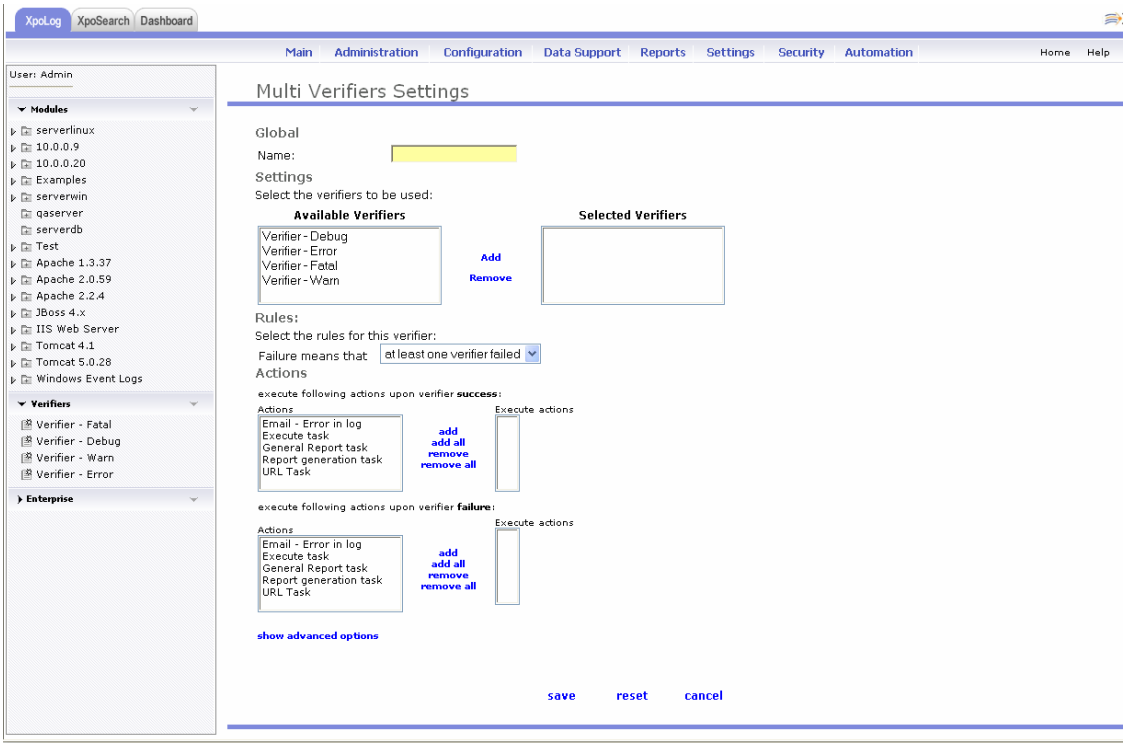
Multi Verifier – multi verifiers is a selection of a few log verifiers all combined into one mechanism.

Specify a name for the multi verifier.

Settings – Add the desired verifiers to the 'Selected' list.

Rules – You may set a rule for the multi verifier, where at least one verifier or **all** verifiers fails, and execute a specific task accordingly.

Actions – add the actions XpoLog should execute in case of failure or success.

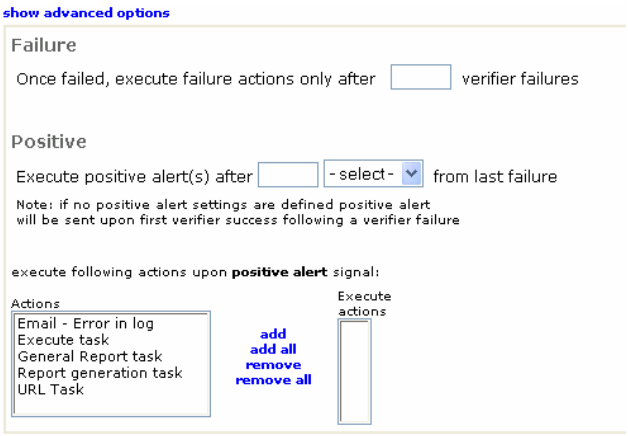


Advanced options – Failure – you can set XpoLog to execute a task upon verifier's failure only after X times it fails, instead of executing this task after each time the verifier fails.

Positive – you can set XpoLog to send a positive alert (A certain task) in 2 ways:

1. Set a time rule – Send a positive alert if the verifier doesn't fail in a certain time frame. I.e. – Send a positive alert 30 minutes after the last verifier's failure.
2. Send a positive alert after the next verifier's success. In that case, the time fields should be left empty.

The last thing you should configure is the task you would like XpoLog to execute as a positive alert.



Click ‘Save’ to finish the multi verifiers wizard.

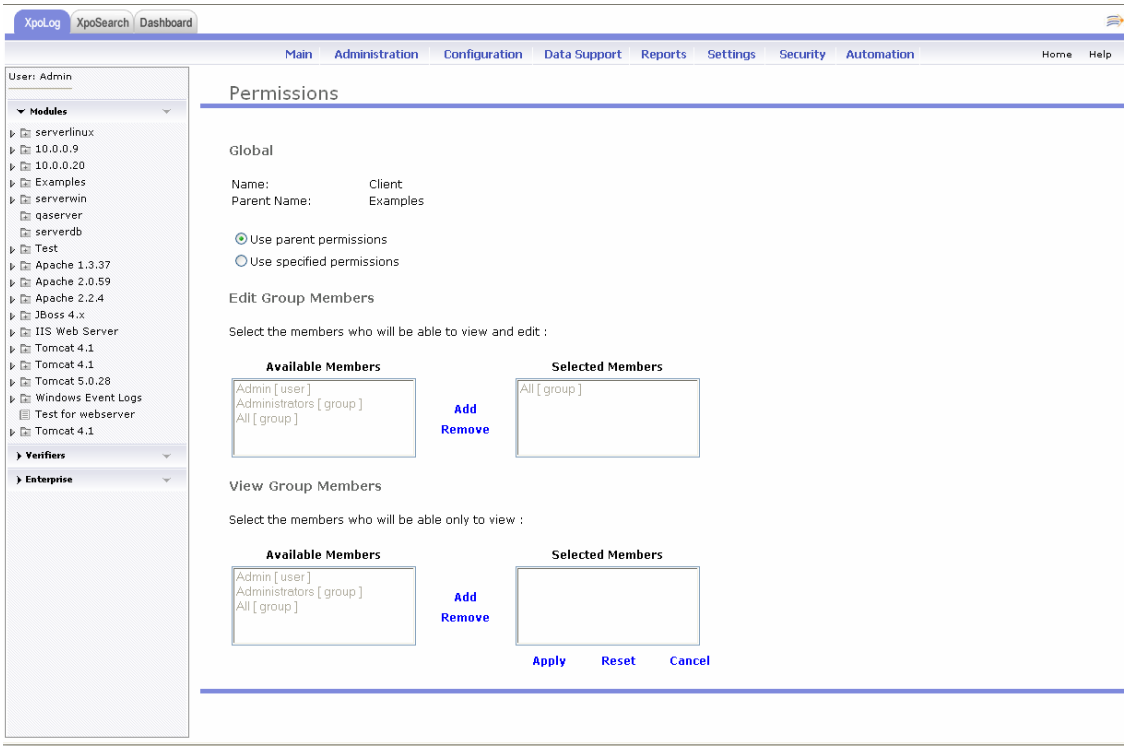
- **Edit verifier**

  In order to edit an existing verifier via the administration menu, the specific verifier should be in focus. Select the relevant verifier in the left pane in the log viewer. When the verifier is in focus, open the administration menu and click ‘Edit verifier’. The verifier’s wizard (Similar to the add verifier wizard) is now available for you to make changes in it. When you are finished editing, click ‘save’.

- **Edit verifier’s permissions**

  Editing the verifier’s permissions enables you to set edit/view permissions for specific users/groups. Editing the verifier’s permissions is only available when security is activated. For further information on security, please refer to Settings → General.

  Select the relevant verifier in the left pane in the log viewer. When the verifier is in focus, open the administration menu and click ‘Edit verifier’s permissions’.



There are two options to set permissions:

1. ‘Parent permissions’ – this will set the same permissions as set in the parent module.
2. ‘Use specified permissions’ – selecting this option will allow you to add or remove users/groups from both available options: Edit group and the View group.

Click ‘Reset’ in case you would like to discard all changes, or click ‘Apply’ in order to save changes.

- **Edit verifier’s Meta data**

  Meta data selection – you can select a Meta data from a list of predefined Meta data schemes. For further information regarding Meta data, please refer to Data support → Meta data.

  Properties – Application: select the most suitable application for the specific log from the list of predefined applications.

  Specify the application version, build, platform, operating system and the vendor.

Add new property – you can add new property to the metadata by clicking ‘add new property’ link. New section will appear, enter the property type and value in the textboxes.

Add menu – you can add new search context by clicking ‘Add menu’ link. New section will appear, enter the search name in the ‘Name’ textbox and the search’s source in the path textbox.

You can use the this metadata by right clicking on the relevant log view, selecting ‘Search’ and choosing the desire search context name.

- **Remove verifier**

  in order to remove a verifier, select the relevant verifier in the left pane in the log viewer, and when the verifier is in focus, open the administration menu and click ‘Remove verifier’. Clicking ‘Ok’ will confirm deletion of verifier. In case you don’t want to delete it, click ‘Cancel’.

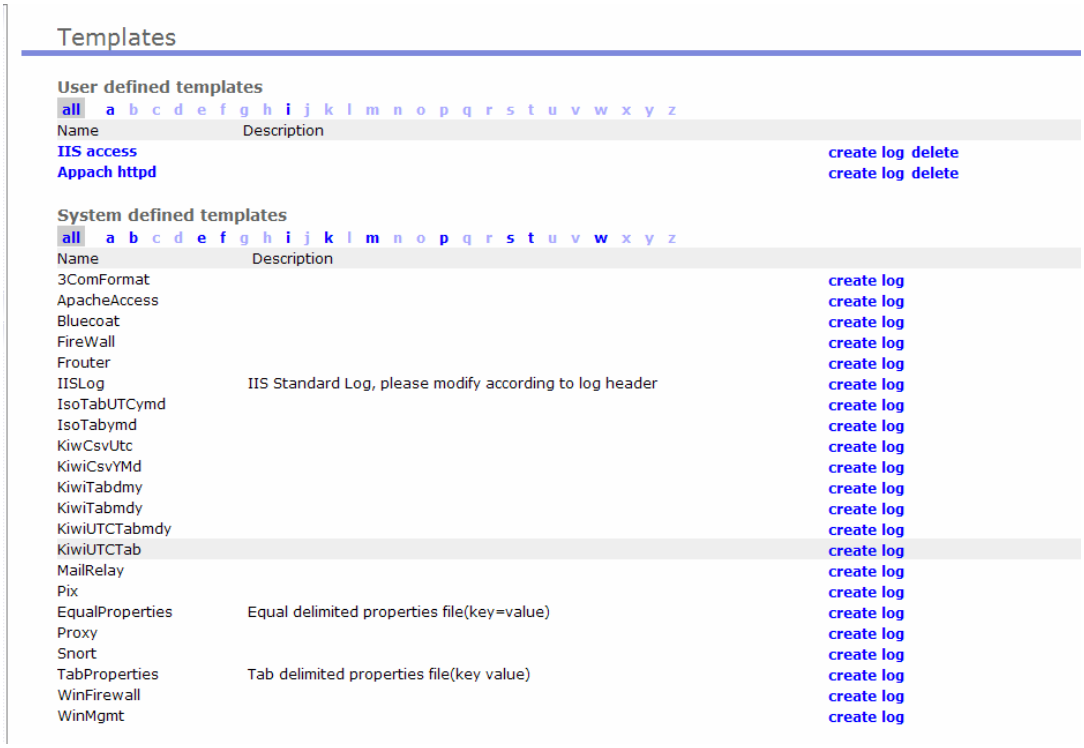
Configuration Menu

Templates

Template is a complete configuration set for a certain file type, enables you to create logs in an easy way.

View Templates

For viewing templates select the 'Configuration' tab in the menu and then click 'View Templates'.



The 'Template' page divided into two sections. 'System defined templates' and 'User defined templates'. 'System defined templates' are predefined configuration integrated with XpoLog software suite.

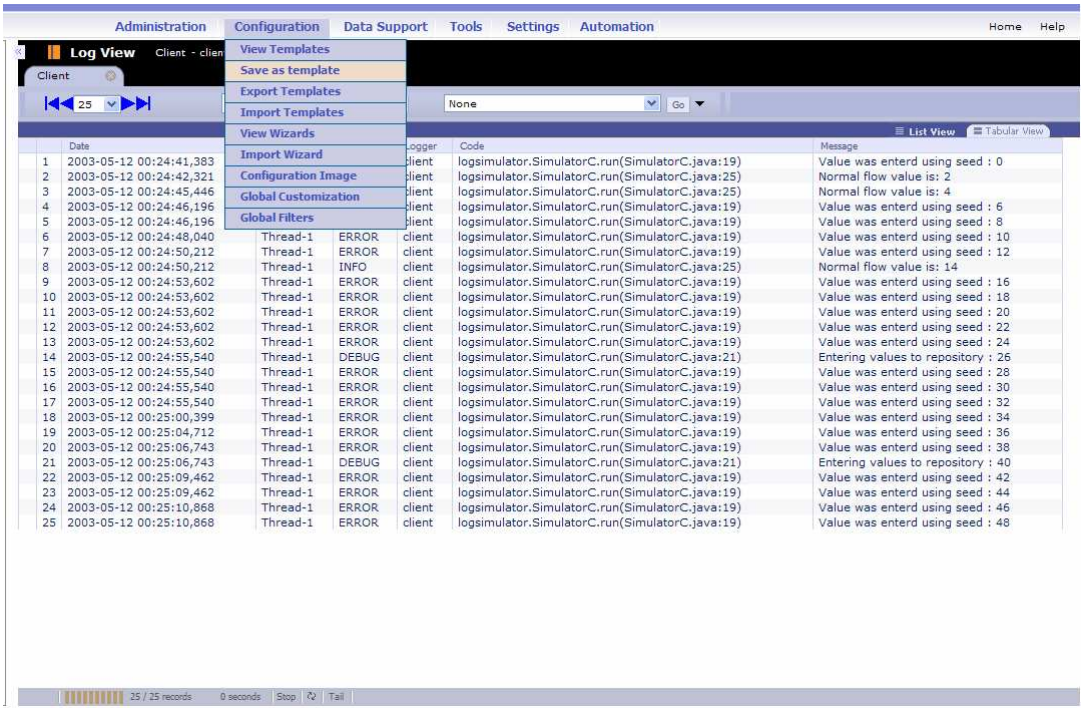
'User defined templates' are configurations sets created by the user.

In each section you can see all defined templates by clicking 'All' in the "ABC" bar or sort those defined templates by clicking the relevant letter.

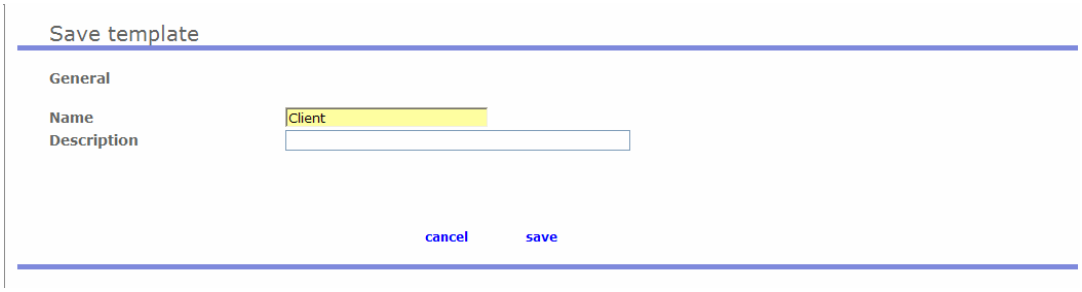
In each section you can see the Template's name and description. For creating the log according to the selected template, click 'create log' link. This link will lead you to create

the log with all the log's definitions within the process (for farther information about creating logs see 'Add Log' section).

Saving a template

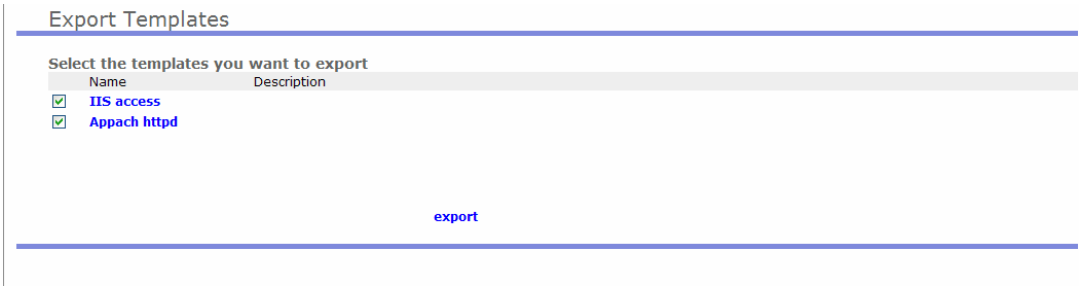


In order to save template, you have to select one log that his properties will be saved as the template. Then select 'Configuration' tab from the menu and click 'Save as template'.



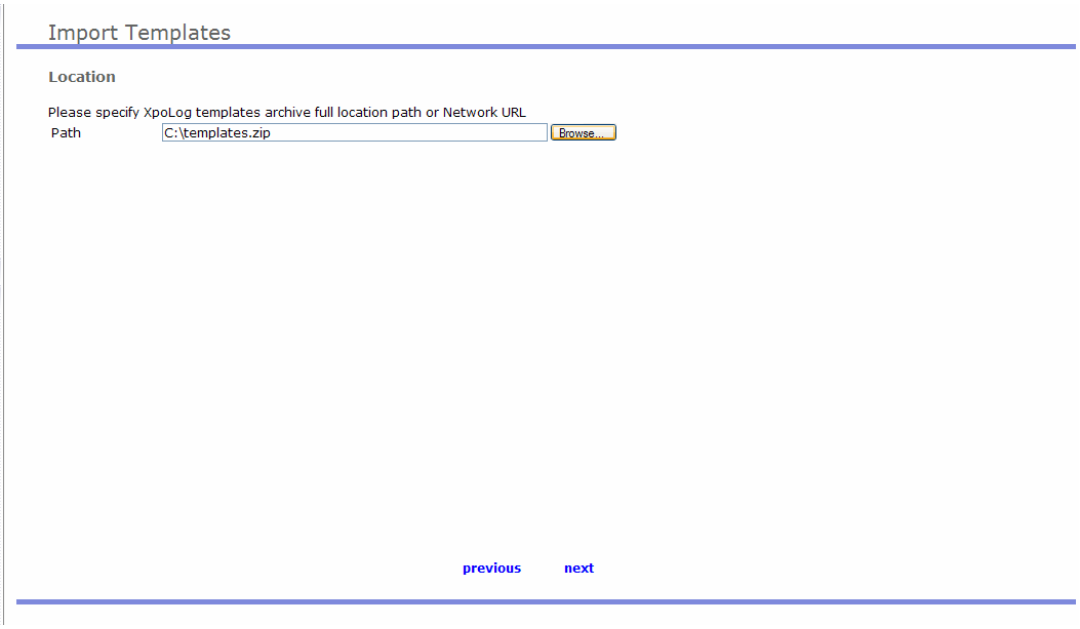
In the 'Name' textbox enter your template name. The default name is the log's name. Enter the description of the template in the 'Description' textbox (Optional). Click 'Save'.

Export Templates



You can export your 'User defined templates' by selecting 'Configuration' and clicking 'Export Templates'. In this page, check the templates you want to export and click 'Export'. Save the zipped file in order to import it latter.

Import Templates



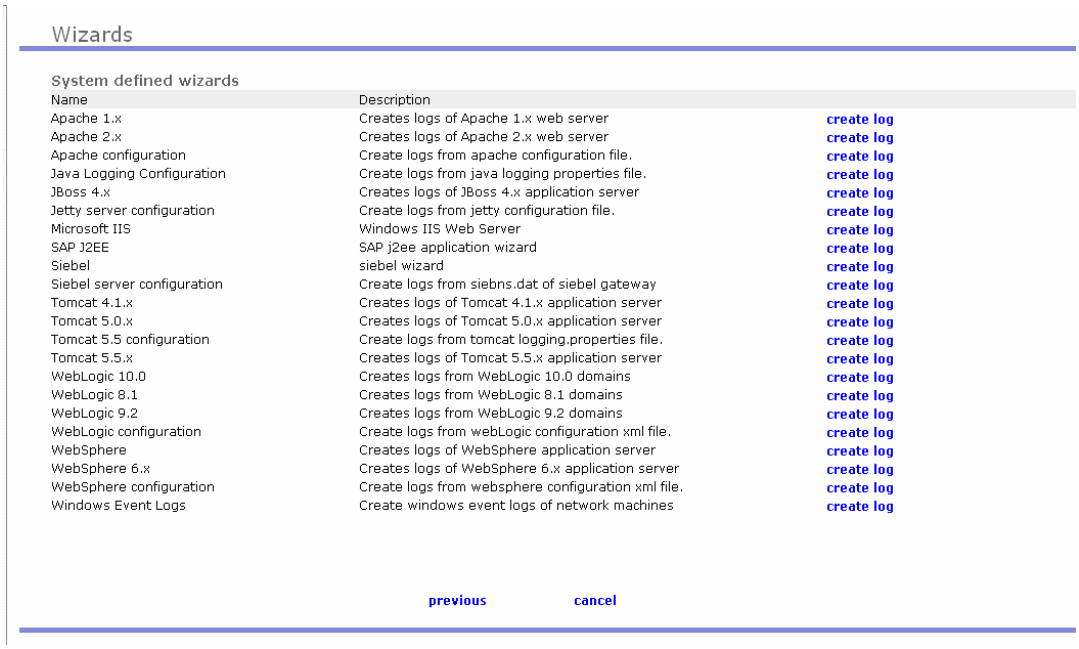
You can import exported templates by selecting 'Configuration' and clicking 'Import Templates'. In this page, browse to the saved zipped file and click 'next'.
The templates were added to your 'User defined templates'.

Wizards

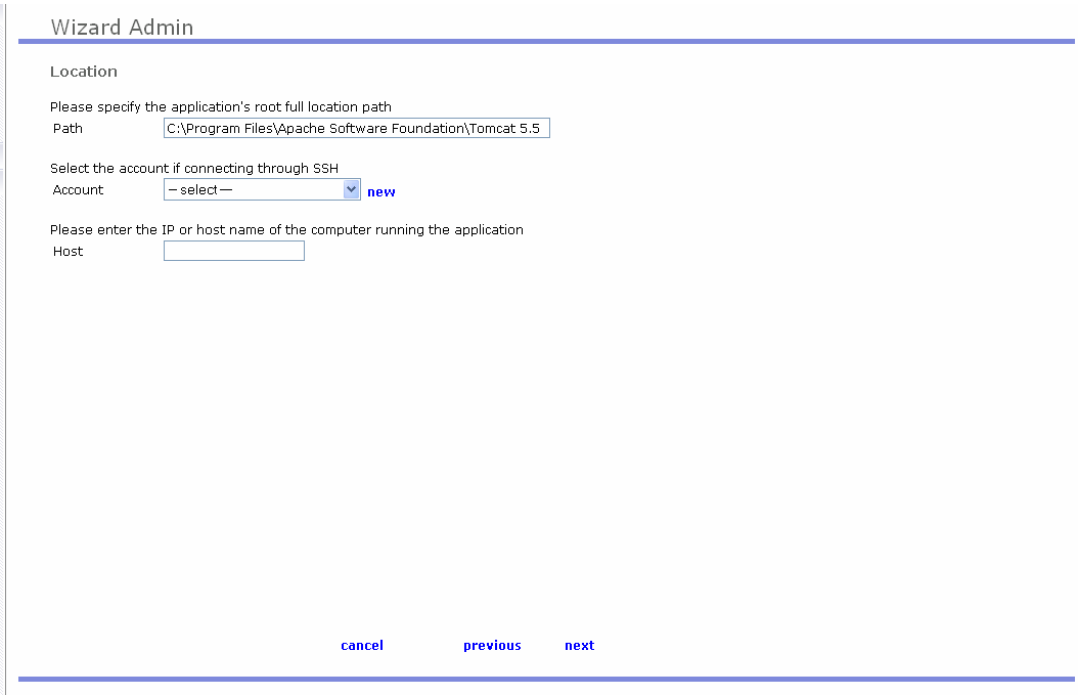
XpoLog comes with a set of wizards that automate the process of adding configuration of modules, logs and reports of known applications to XpoLog.

View Wizards

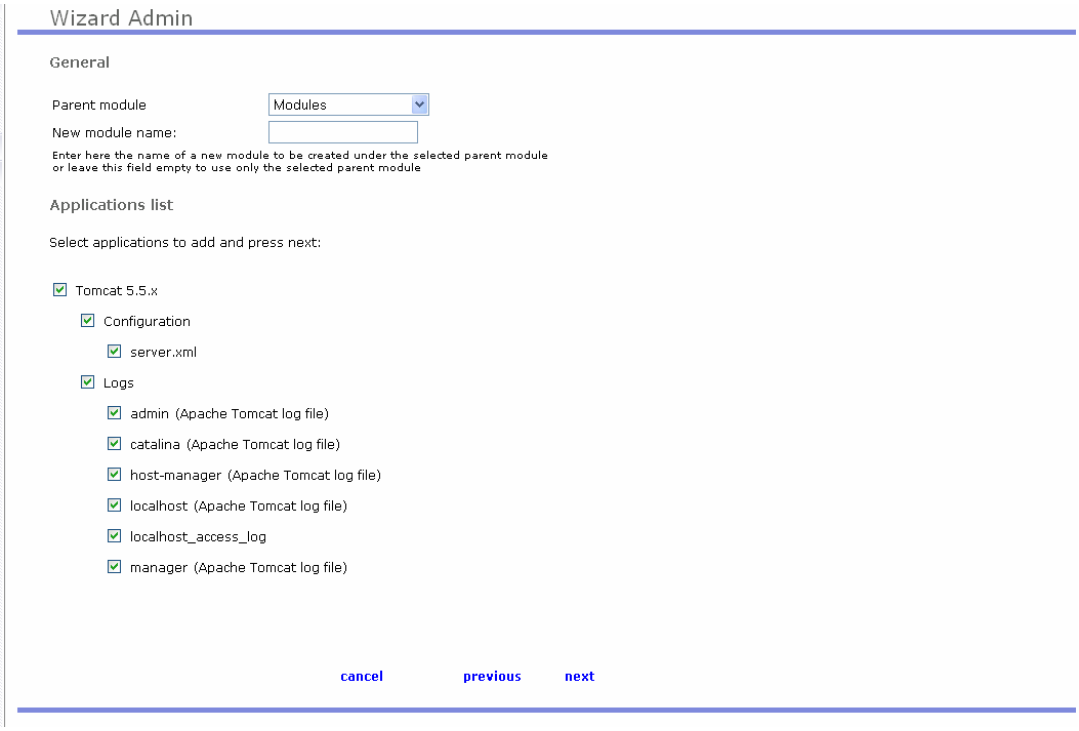
For viewing the wizards select the 'Configuration' tab in the menu and then click 'View Wizards'.



In order to create the modules, logs and reports for the desire application, click ‘create log’ link.



In the ‘Path’ textbox fill the application’s root full location path. In case the wizard detected the application it will fill this textbox with the default application’s path.
If you connected to the selected application through SSH connection or win authentication account, select the account from ‘Account’ select box or create new account. For further information regarding SSH and Windows authentication accounts, please refer to Data support → Address book.
If the selected application runs on remote machine, fill his IP or host name in the ‘Host’ textbox. Click ‘next’.



In ‘Wizard Admin’ page, select the parent module for your selected modules and logs from 'Parent module' select box. By default to root module "Modules" is selected.
In 'New module name' enter the name of a new module to be created or leave this field empty to use only the selected parent module. Click 'next' to end this process.

Import Wizards

For import wizard select the 'Configuration' tab in the menu and then click 'Import Wizard'.

Browse to the wizard's zip file and click 'next'.

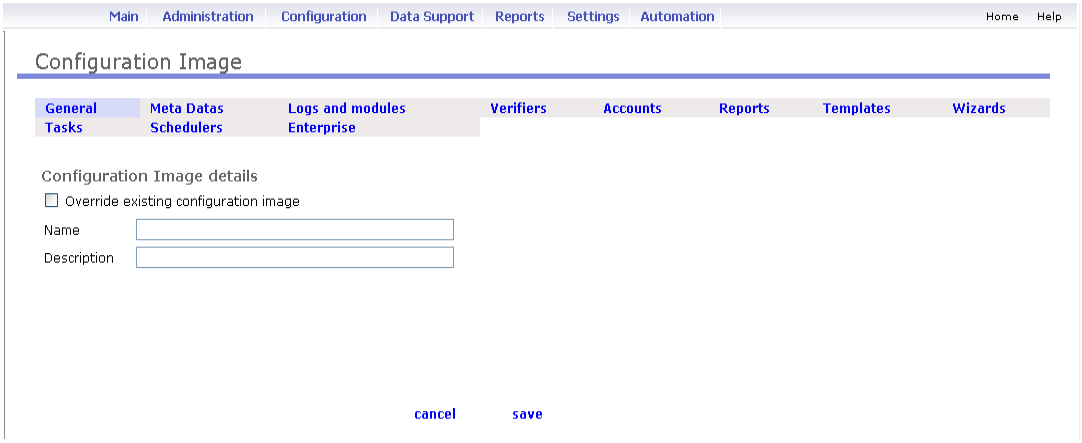
Configuration Image

A configuration image is the description of a set of XpoLog components, such as logs, reports, verifiers and so on. A configuration image can be exported and saved in the file system and could be later imported to created an identical configuration to the one that was saved.

From 'Configuration' menu select 'Configuration Image'

Add New Configuration Image:

To add new 'Configuration Image' click on 'Add new Configuration Image'.



In the 'Name' text box enter your configuration image name. In the 'Description' text box enter its description (optional).

You can override existing configuration images by checking the 'Override existing configuration image' checkbox.

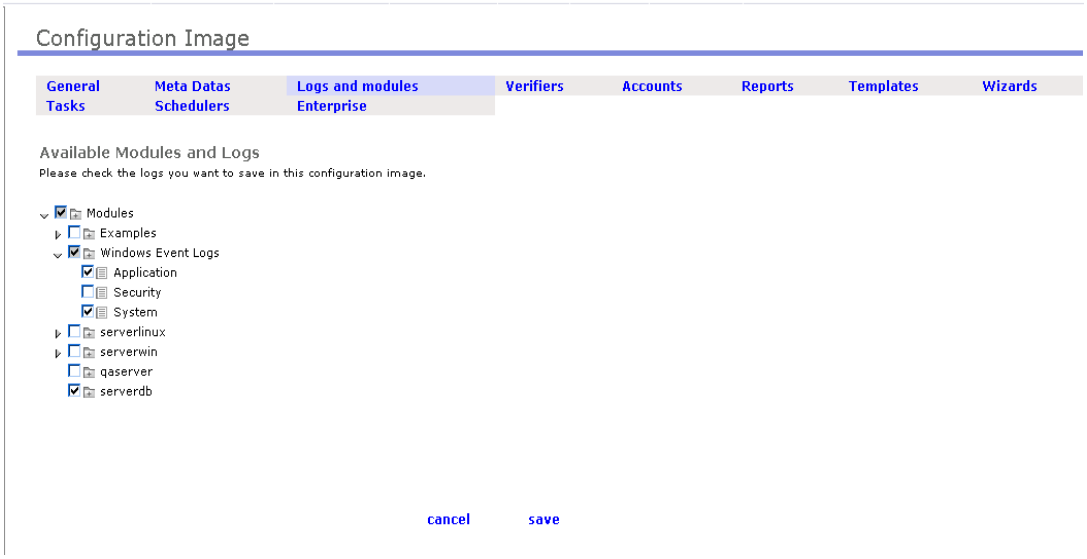
You can save your configuration image any time you want by clicking the 'save' link or 'Cancel' to go back to 'configuration Image' main page.

Adding Meta data configuration to your configuration image:

Select 'Meta Data' tab from menu and then select the desirable Meta data.

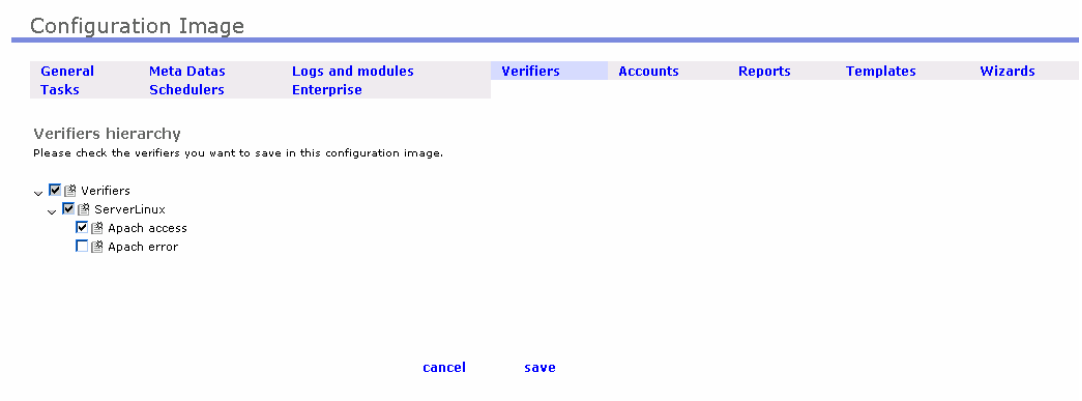
Adding logs and modules configurations to your configuration image:

Select 'Logs and Modules' tab from menu and then select the desirable logs and modules.



Adding verifiers' configurations to your configuration image:

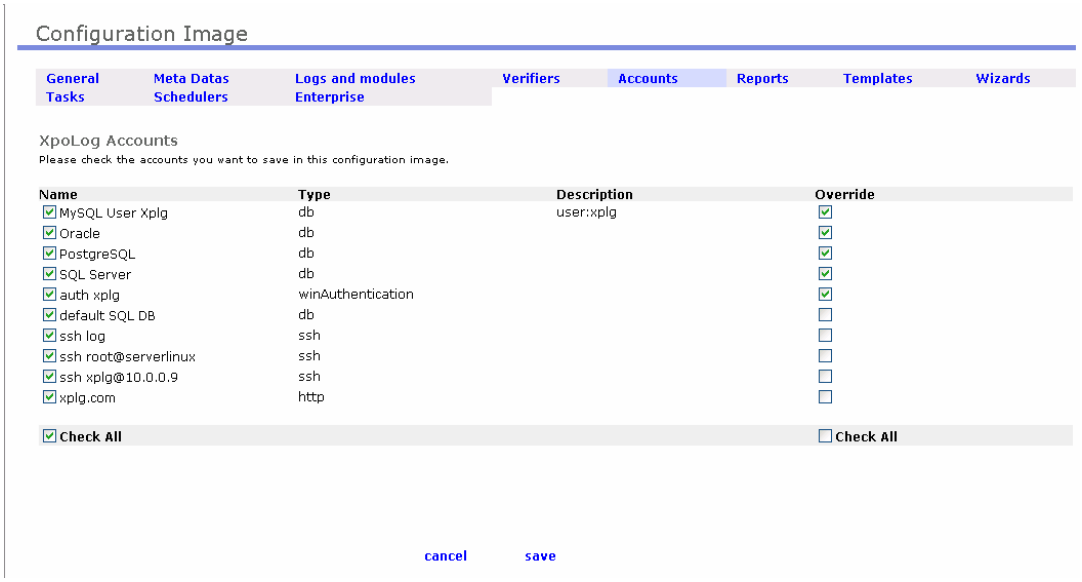
Select 'Verifiers' tab from menu and then select the desirable verifiers and multi-verifiers.



Adding accounts configurations to your configuration image:

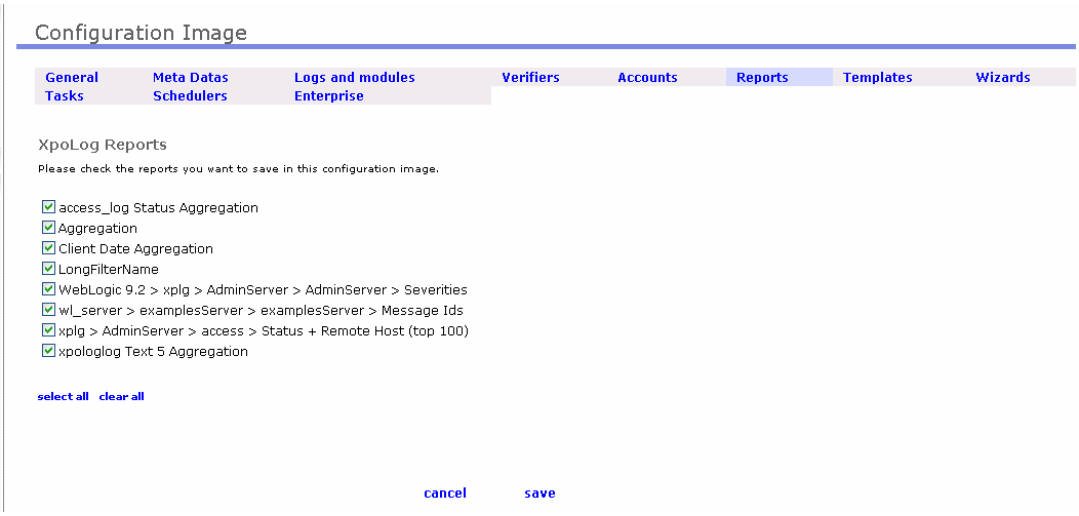
Select 'Accounts' tab from menu and then select the desirable accounts.

If you check the checkbox in the 'Override' column, the correlate accounts configuration will override the identical account configuration (if exist).



Adding reports configurations to your configuration image:

Select 'Reports' tab from menu and then select the desirable reports.



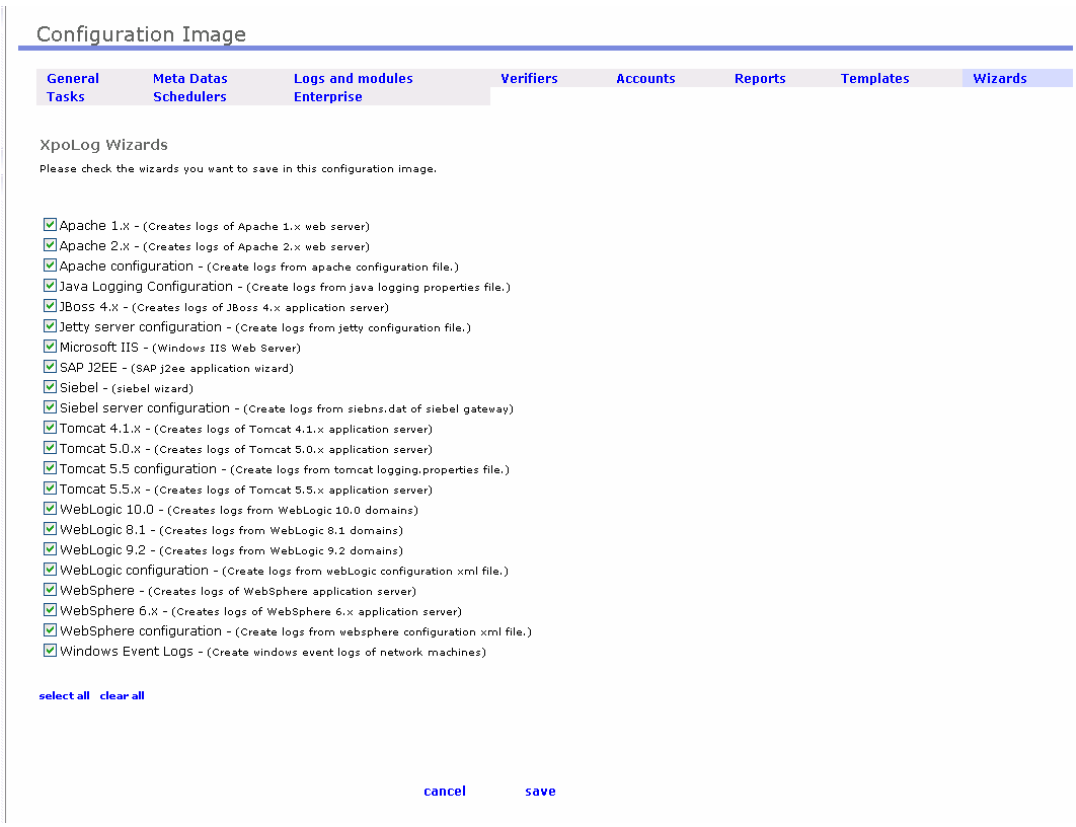
Adding templates configurations to your configuration image:

Select 'Templates' tab from menu and then select the desirable templates.

You can select 'User defined templates' that are templates that were created by the user and 'System templates' that are default templates added to the system.

Adding wizards' configurations to your configuration image:

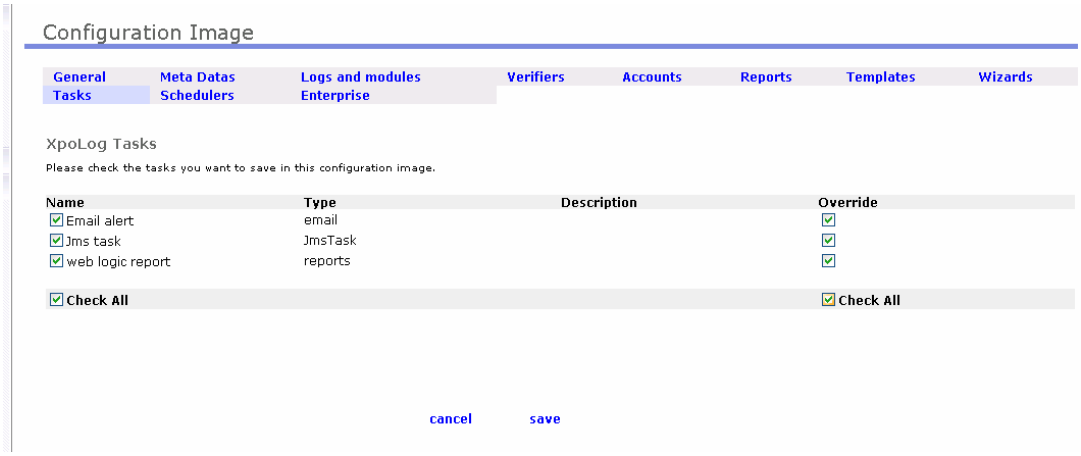
Select 'Wizards' tab from menu and then select the desirable wizards.



Adding tasks configurations to your configuration image:

Select 'Tasks' tab from menu and then select the desirable tasks.

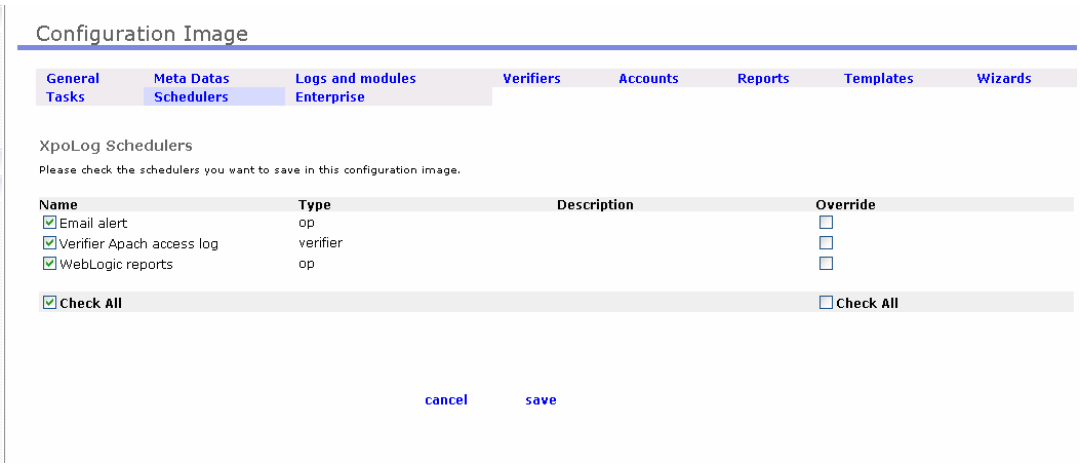
If you check the checkbox in the 'Override' column, the correlate task configuration will override the identical task configuration (if exist).



Adding schedulers' configurations to your configuration image:

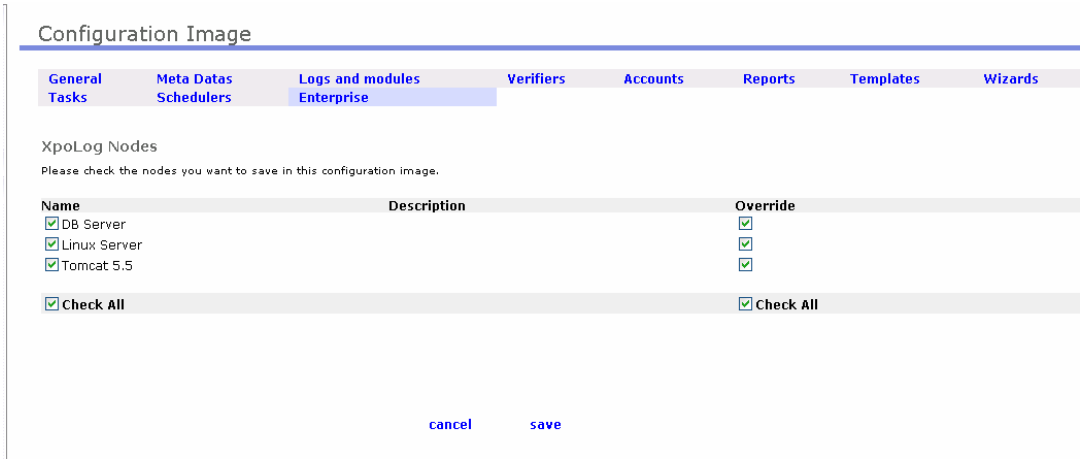
Select 'Schedulers' tab from menu and then select the desirable schedulers.

If you check the checkbox in the 'Override' column, the correlate scheduler configuration will override the identical scheduler configuration (if exist).



Adding enterprises configurations to your configuration image:

Select 'Enterprises' tab from menu and then select the desirable enterprises.

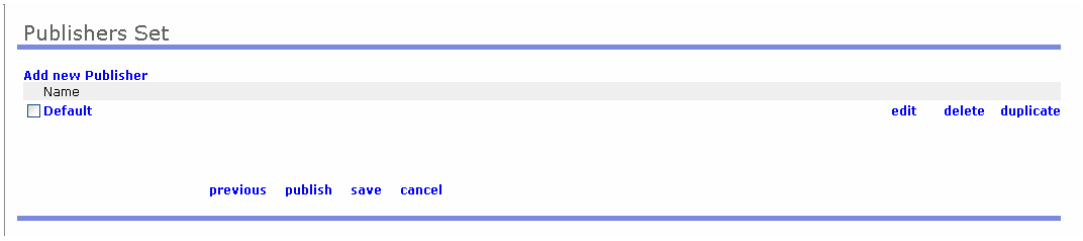


If you already have a configuration image you can edit, duplicate or delete it by clicking the matching links.

Publish existing Configuration Image

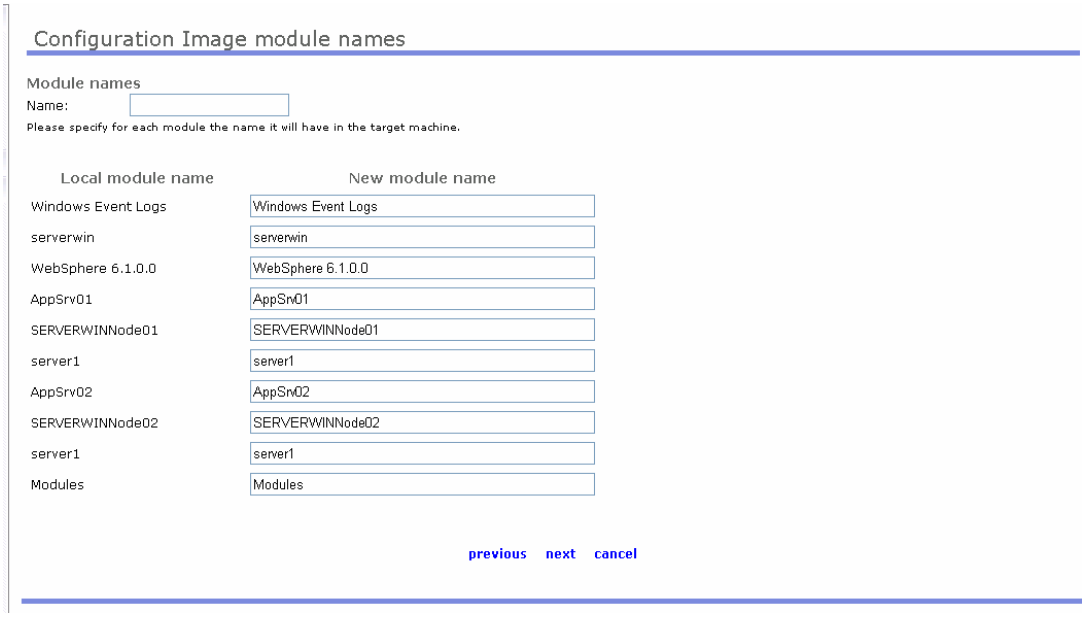
The publish action allows you to publish an existing configuration image to other XpoLog node or to your local XpoLog node.

Do that by clicking on the 'Publish' link.

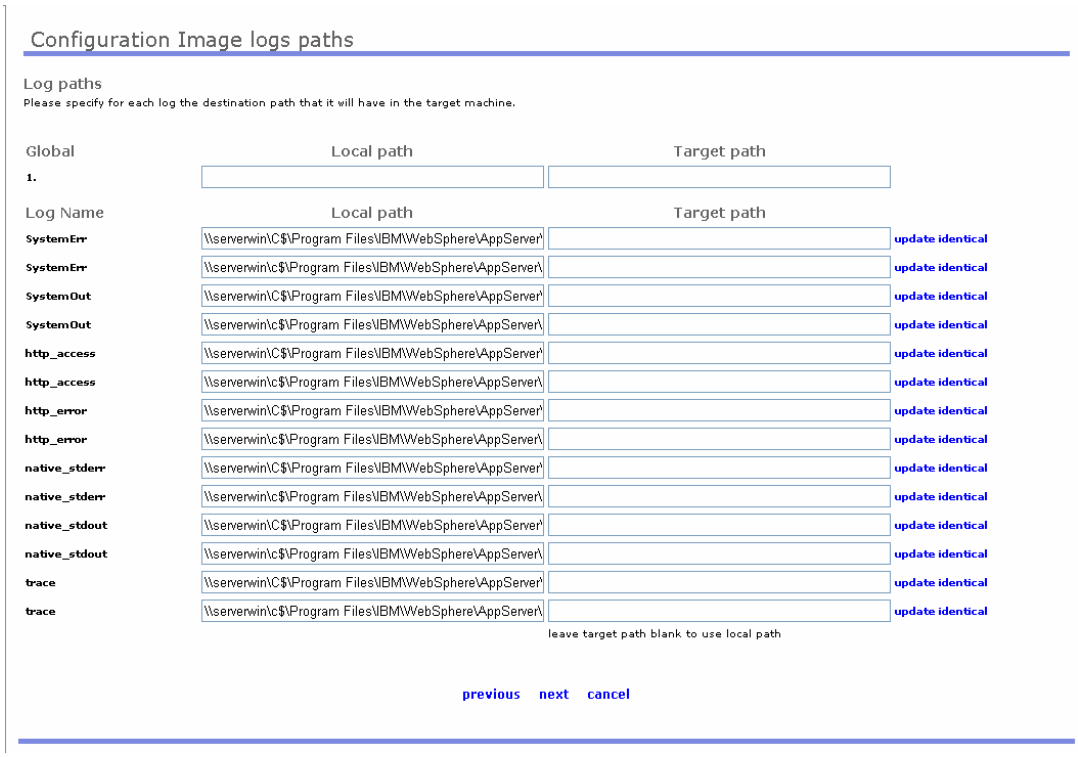


If you want to use the default publisher, check the 'Default' checkbox. You can also edit, delete or duplicate this publisher by clicking the matching link.

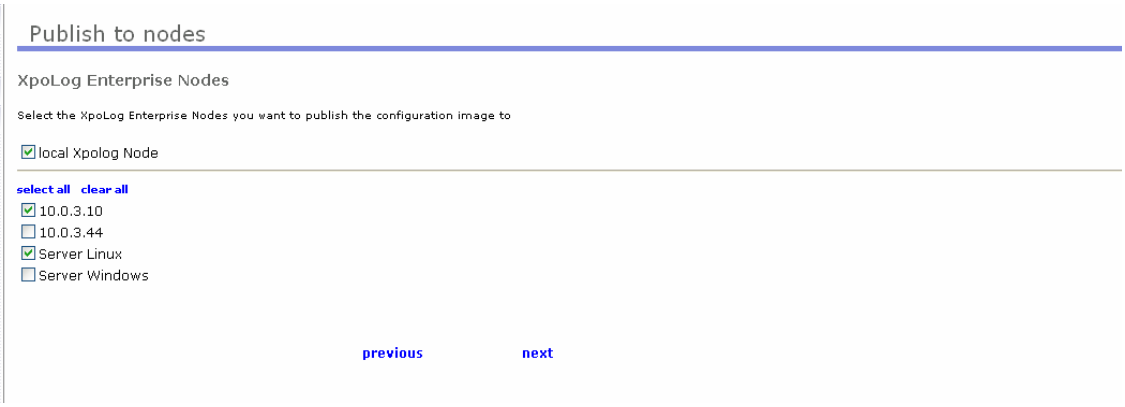
In order to create new publisher click the 'Add new Publisher' link.



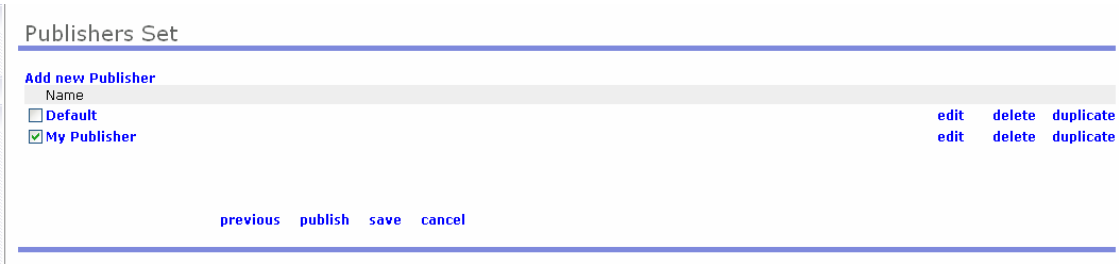
In the 'Name' textbox enter the publisher's name. For each (local) module you can give new name that will be assigned while importing. Click 'Next'.



In The logs paths page you can change the target logs paths. In the 'Global' section you can give a local global path, that all the local logs located in that path, will get new path at the target machine. Enter the new target path in the 'Target path' textbox.
You can do the same action for each log separately at the 'Log Name' section. Click 'Next'.



In 'Publish to nodes' page you decide to which nodes you want to publish the configuration image. Check the 'local XpoLog Node' checkbox if you want to publish this image to your local machine. Check any other enterprise nodes (if exist) for remote publishing. Click 'Next'.

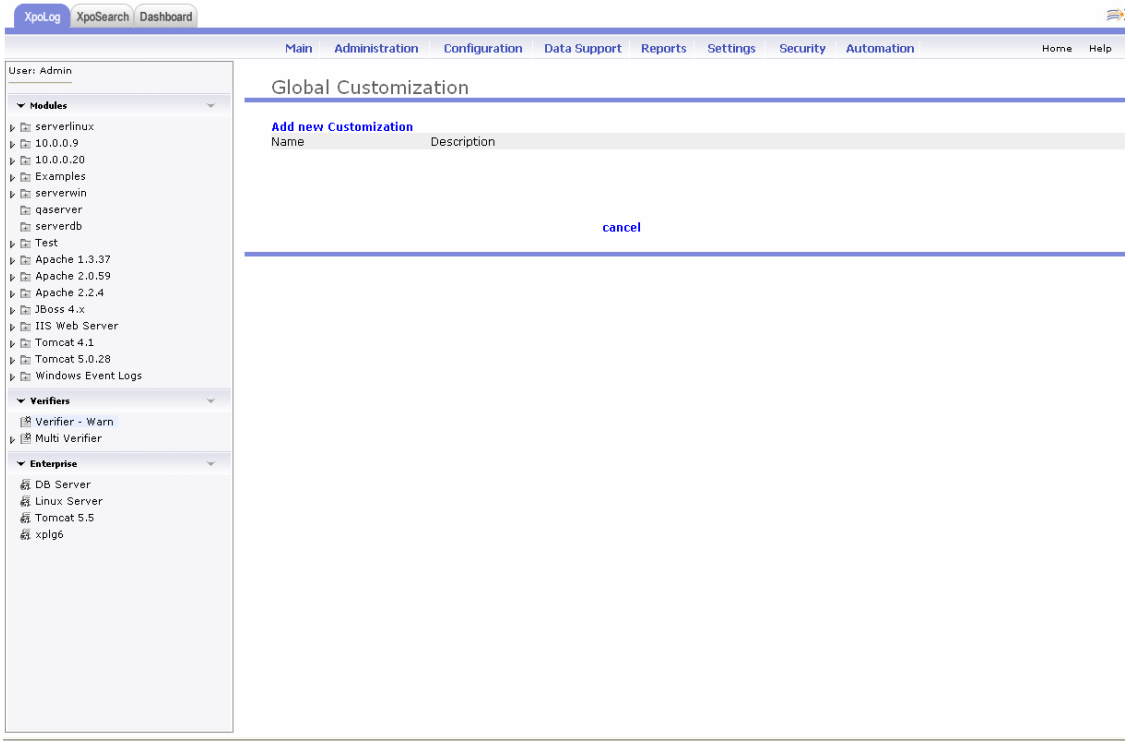


Select the publisher you want to use by checking its checkbox and then click 'Save' to save the publisher definition or click 'Publish' for publishing the configuration image by the selected publisher.

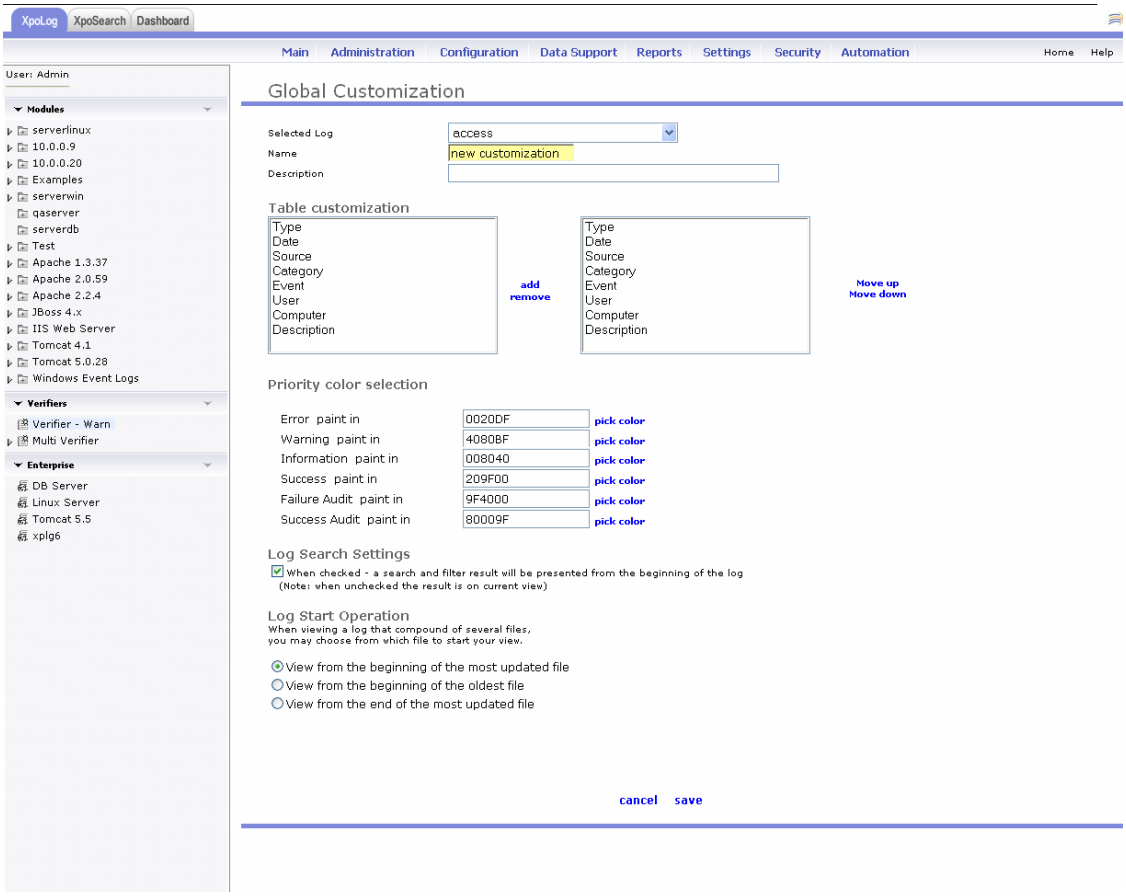
Global Customization

Add new customization - Global customization allows you to change a few general logs settings, such as table customizing, color selection and log view options.

To add a new global customization, from the configuration menu select ‘Global customization’



Click ‘Add new customization’ in order to start the wizard.

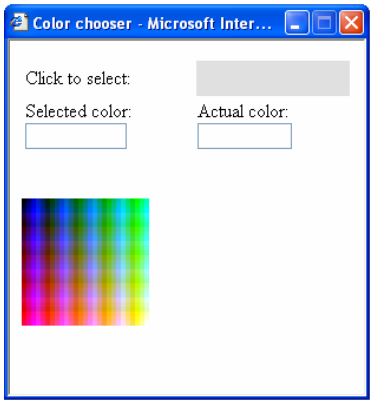


First of all, select the log you wish to customize from the list of the available logs in XpoLog.

Specify a name and description for the customization.

Table customization – you may add or remove columns from the log, and you can set their order by moving them up/down.

Priority color selection – you can select the color of each one of the priorities in the list, by clicking the 'Pick color' link, and choosing the desired color.



Log search settings - check this option in case you would like XpoLog to present a search and filter result from the beginning of the log

Log start operation - In case a log is compound of more then one file, you may select the file display order as following:

View from the beginning of the most updated file

View from the beginning of the oldest file

View from the end of the most updated file

Click ‘save’ when done configuring the log’s customization, or ‘cancel’ to discard changes.

Edit global customization

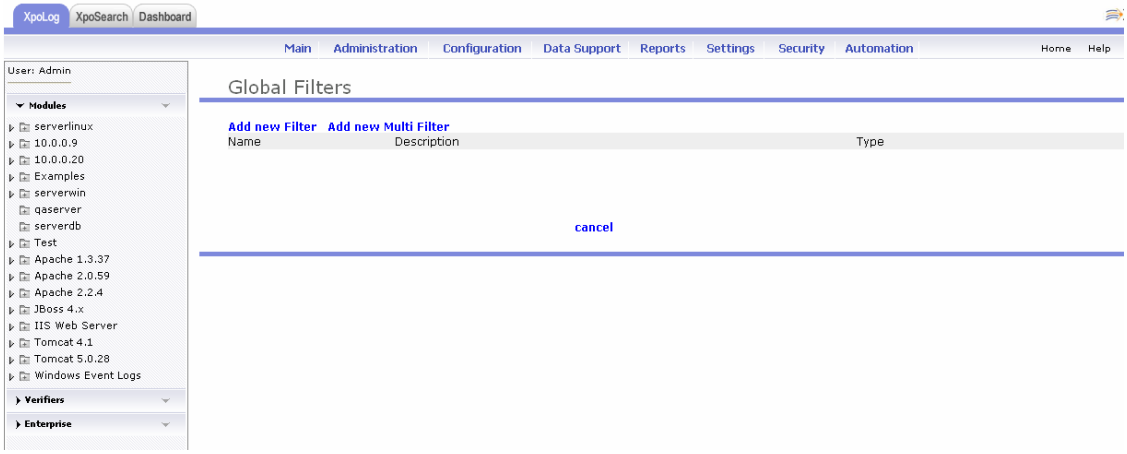
The global customizations can be edited in the future. Click ‘Global customization’ in the configuration menu, and click ‘edit’ next to the customization you wish to edit.

Delete global customization

In case you would like to remove a global customization, click the ‘delete’ link opposite to the relevant customization name.

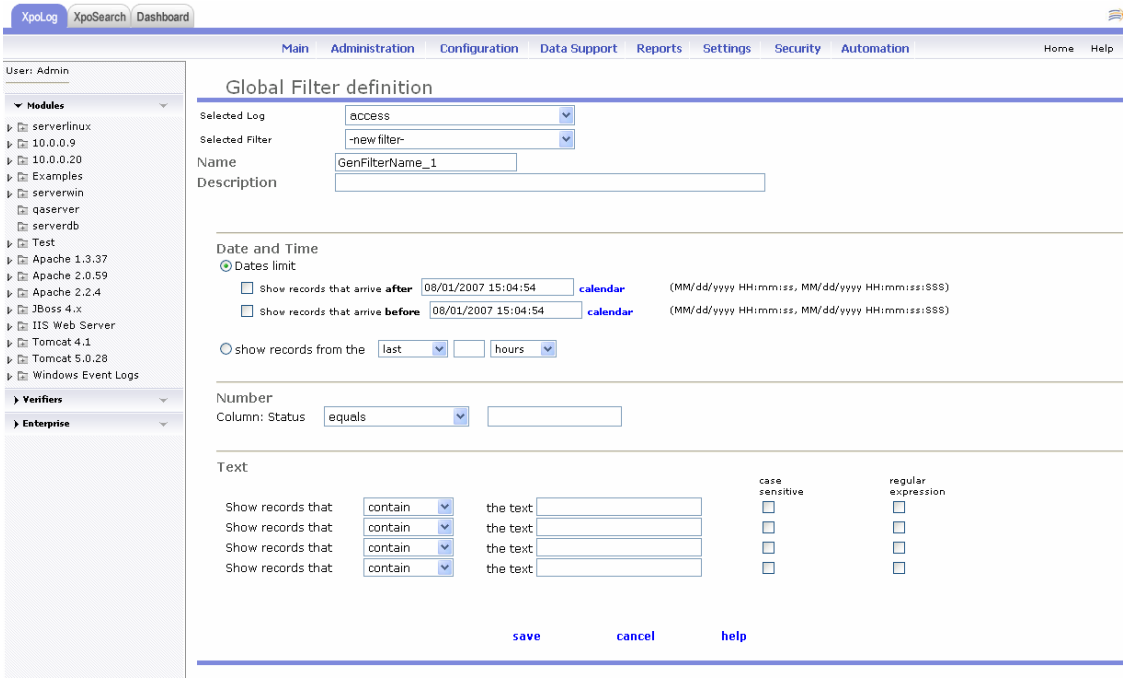
Global Filters

A global filter enables you to create a single filter that will be available for all logs using the same log pattern. This feature saves you the time of creating dozens of regular filters for every log, when all these logs are using the same pattern.



There are 2 different kinds of global filters: **Global filters** and **Multi filters**.

Add new global filter – Select the log you wish to create a global filter to from the list of XpoLog's logs. The whole wizard will refresh according to the selected log. You may select one of the log's predefined filters, and the wizard will update itself according to the specific filter's properties.



In case you would like to create a new filter, please specify a name and description to the new filter.

Date and time – you may set date limits for the filter, using the ‘dates limit’ fields, or leave it blank and not limit the filter at all.

Number/Text – in these fields you should add the relevant information you would like to filter from the specific log.

When you finished configuring the global filter, click ‘Save’ or click ‘Cancel’ to discard changes.

Add new multi global filter

The multi filter is combination of a few global filters.

Click the ‘add new multi filter’

Specify a name and description for the new multi filter.

From the list of available filters add at least two filters, and specify the logical operation (or/and) between those filters.

Edit global filter/Multi filter

The global filter/multi filter can be edited at any time. Click ‘Global filter’ in the configuration menu, and click ‘edit’ next to the filter/multi filter you wish to edit.

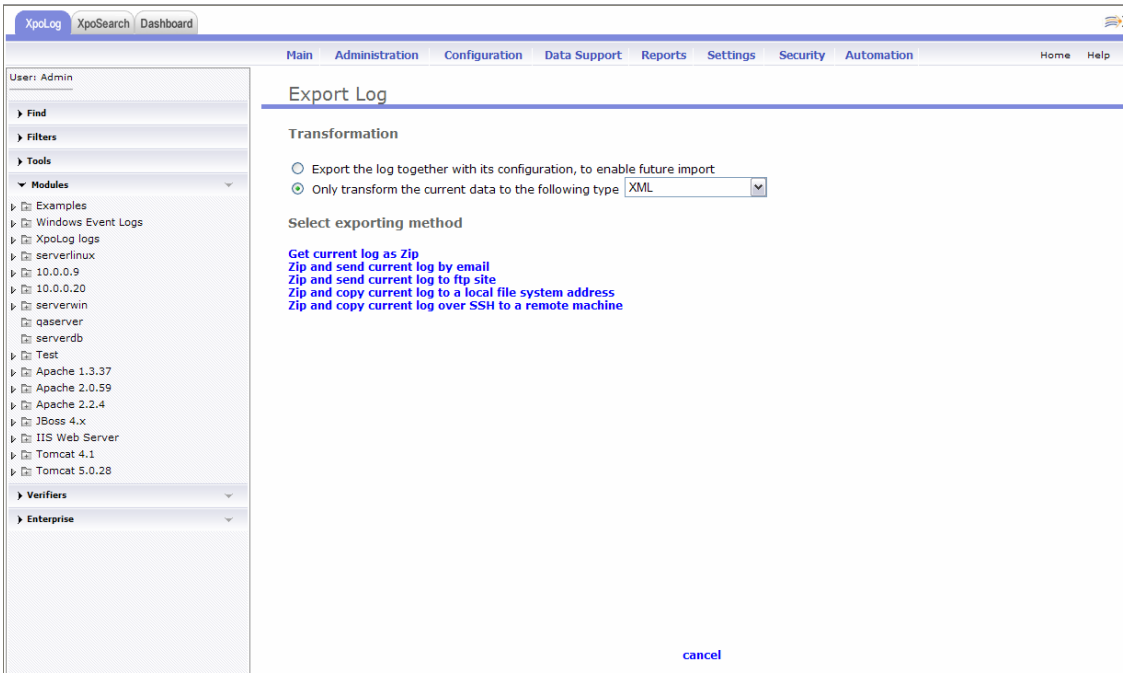
Click ‘save’ when done or ‘cancel’ to discard changes.

Delete global customization

In case you would like to remove a global filter/multi filter, click the ‘delete’ link opposite to the relevant filter/multi filter’s name.

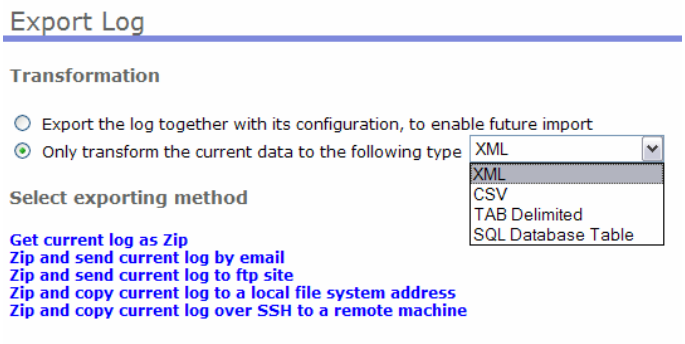
Data Support Menu

Export Log



All logs can be exported from XpoLog in one of the two following ways:

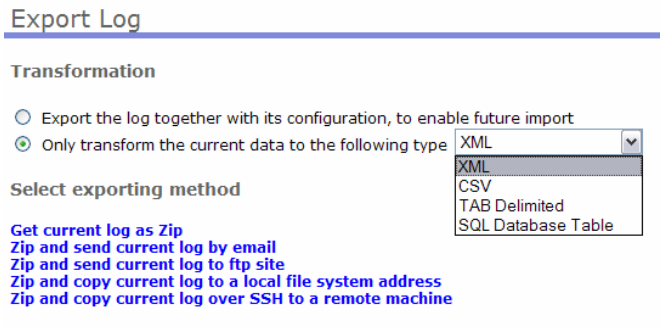
1. The log is exported with its configuration, in case you would like to import it again in the future.
2. Only the log's data is exported. The log's configuration will be lost. There are 4 different types you can transform the current data to: XML, CSV, Tab Delimited, and SQL DB table.



In order to export a log, select the relevant log in the left pane in the log viewer, and when the log is in focus, open the data support menu, and select the export log option. Choose the desired transformation type (With or without the log's configuration), and click the desired exporting method, from the following available options:

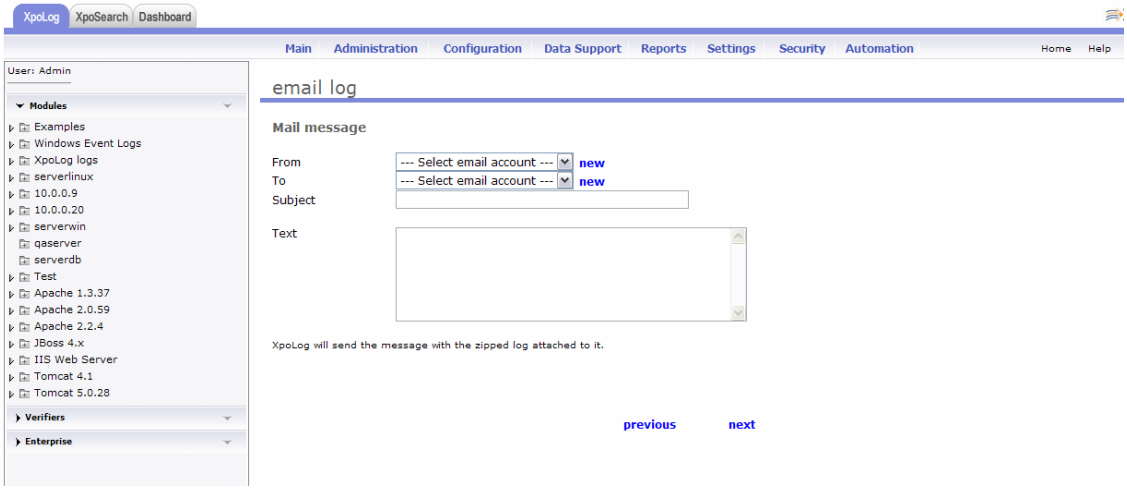
Get current log as zip

Selecting this option will save the current log as a zip file. You can open the zip file or save it for future use.



Zip and send current log by email

The log will be sent via email, as a zip file.



Select an email account for both the sender and the receiver of this email, from the list of the predefined email accounts, or create a new email account by clicking ‘new’. For further information regarding email accounts, please refer to Data support → Address book.

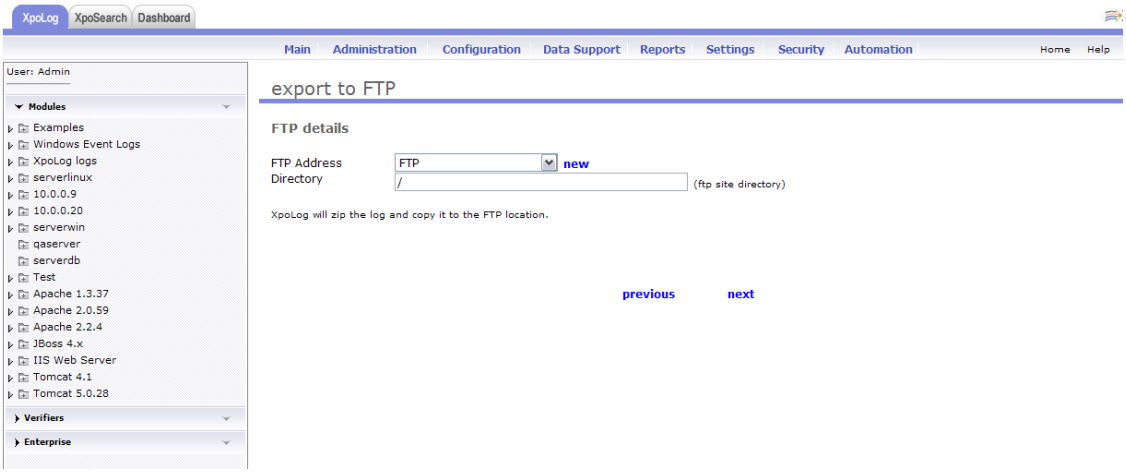
Add a subject for this email, and add text if required. Click ‘next’ in order to send the email.

Zip and send current log to an FTP site

The log will be sent to an FTP site.

In the FTP address, select an FTP account, or click ‘new’ in order to configure a new one. For further information regarding FTP accounts, please refer to Data support → Address book.

Specify the FTP site directory, in which the log will be saved, and click ‘next’ to start the transfer process.



Zip and copy current log to a local FS address

The log will be copied to a local file system address on your machine. From the 'Directory' combo box select the FS account you wish to save the log to, or click 'new' in order to configure a new FS account. For further information regarding FS accounts, please refer to Data support → Address book.

Check the 'Overwrite' option in case you would like XpoLog to overwrite an existing similar file.

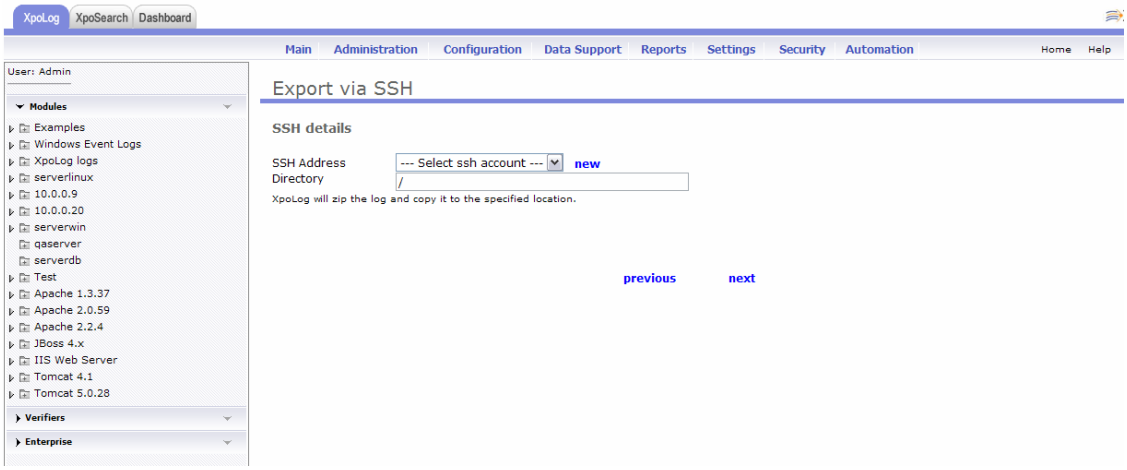
Click 'next' to start the transfer process.

Zip and copy current log over SSH to a remote machine

The log will be transferred over SSH to a remote machine. Select an SSH account from the list of available SSH accounts, or click new in order to configure a new SSH account. For further information regarding SSH accounts, please refer to Data Support → Address book.

Specify the directory on the remote machine, in which XpoLog will copy the log to.

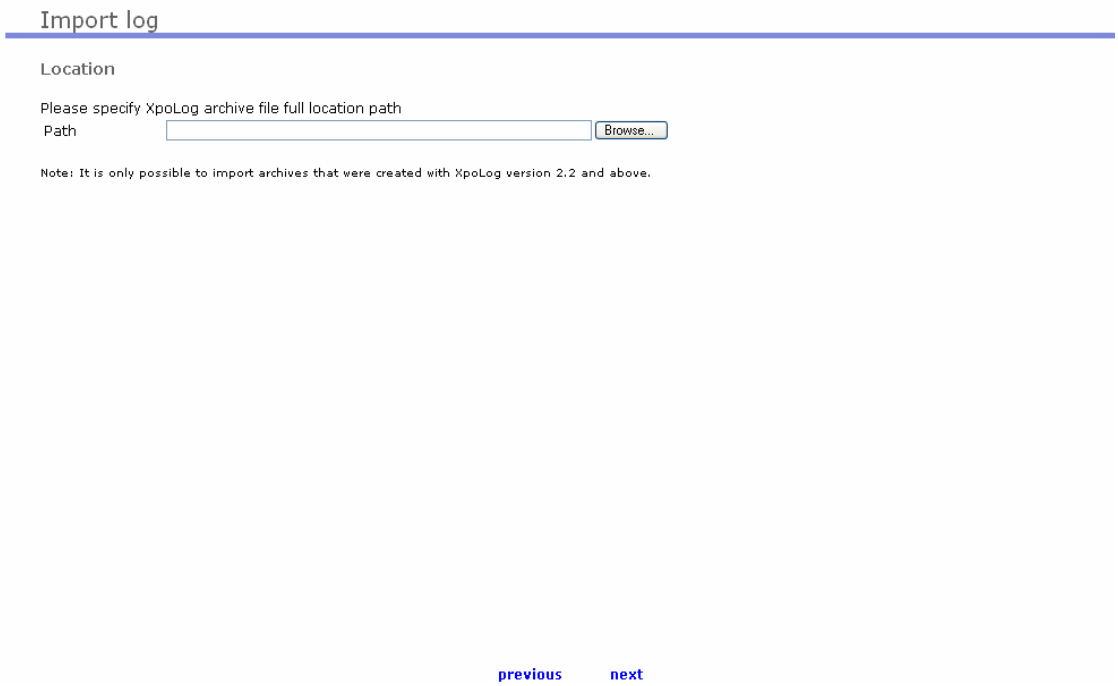
Click 'next' to start the transfer over SSH process.


XpoLog
XpoSearch
Dashboard
Main
Administration
Configuration
Data Support
Reports
Settings
Security
Automation
Home
Help
User: Admin
Modules
Examples
Windows Event Logs
XpoLog logs
serverlinux
10.0.0.9
10.0.0.20
serverwin
qaserver
serverdb
Test
Apache 1.3.37
Apache 2.0.59
Apache 2.2.4
JBoss 4.x
IIS Web Server
Tomcat 4.1
Tomcat 5.0.28
Verifiers
Enterprise
Export via SSH
SSH details
SSH Address
--- Select ssh account ---
new
Directory
/
XpoLog will zip the log and copy it to the specified location.
previous
next

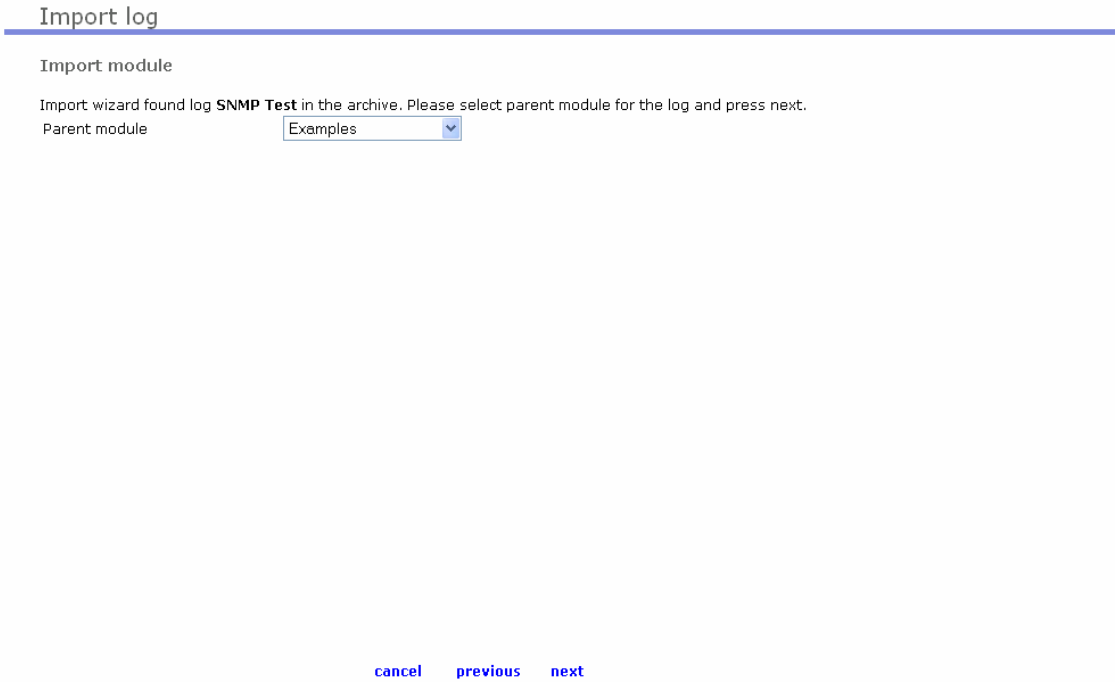
Import Log

You can import to XpoLog any kind of log, as long as it was exported with its configuration.

Specify the log's path, and click 'Next'.

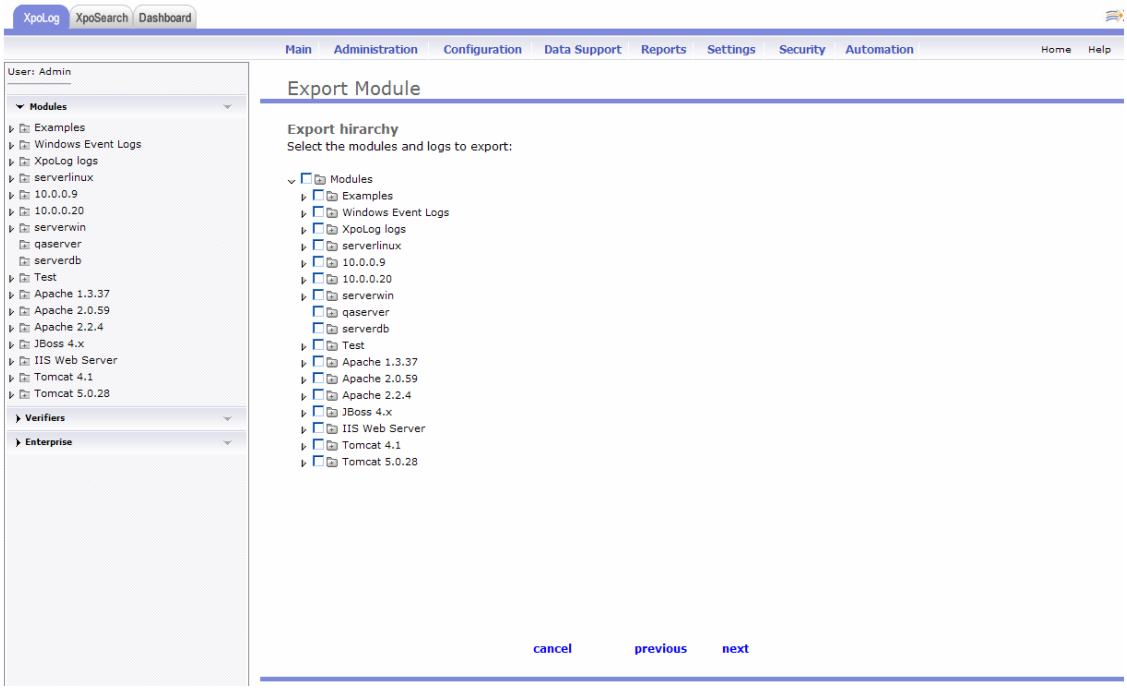


After finding the desired log, please select a parent module from the list of available modules.

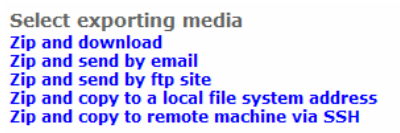


Click ‘next’ to finish the import process or ‘previous’ in case you would like to import a different log. Click ‘Ok’ to confirm the successful import.

Export Module



In order to export a module from XpoLog, make your selection in XpoLog module's tree, and click 'Next'. There are five different export methods to choose from:

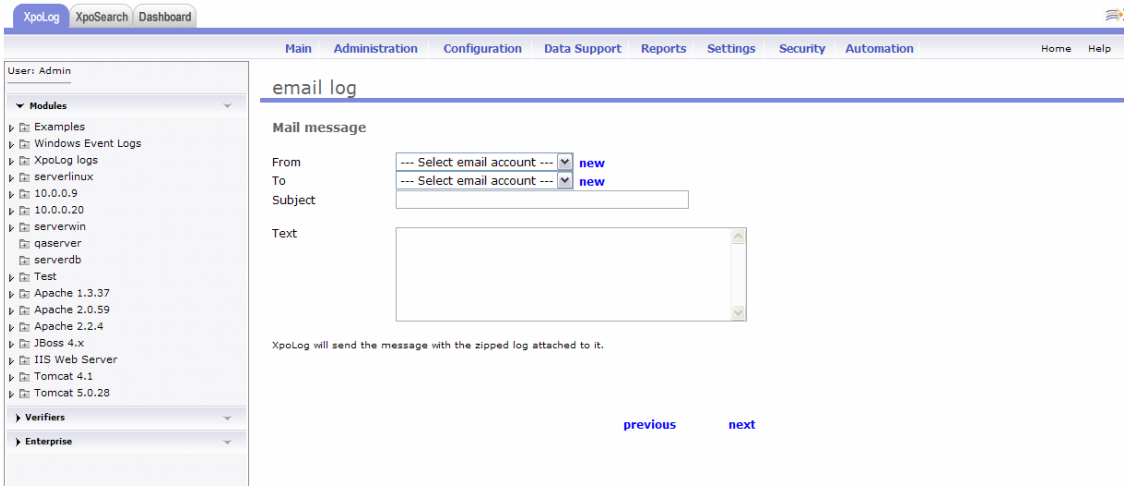


Zip and download

Selecting this option will save the current module as a zip file. You can open the zip file or save it for future use.

Zip and send by email

The module will be sent via email, as a zip file.



Select an email account for both the sender and the receiver of this email, from the list of the predefined email accounts, or create a new email account by clicking ‘new’. For further information regarding email accounts, please refer to Data support → Address book.

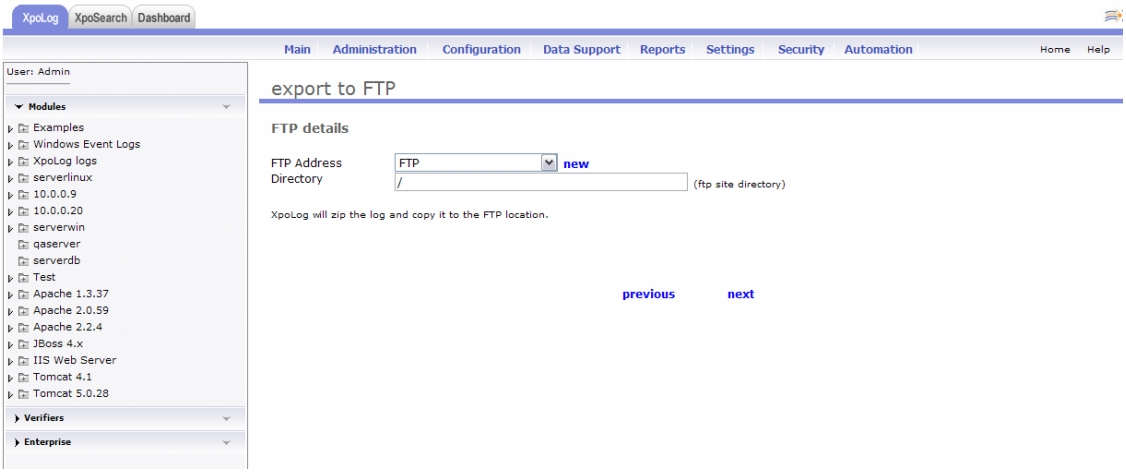
Add a subject for this email, and add text if required. Click ‘next’ in order to send the email.

Zip and send to an FTP site

The module will be sent to an FTP site.

In the FTP address, select an FTP account, or click ‘new’ in order to configure a new one. For further information regarding FTP accounts, please refer to Data support → Address book.

Specify the FTP site directory, in which the module will be saved, and click ‘next’ to start the transfer process.



Zip and copy to a local FS address

The module will be copied to a local file system address on your machine. From the 'Directory' combo box select the FS account you wish to save the module to, or click 'new' in order to configure a new FS account. For further information regarding FS accounts, please refer to Data support → Address book.

Check the 'Overwrite' option in case you would like XpoLog to overwrite an existing similar file.

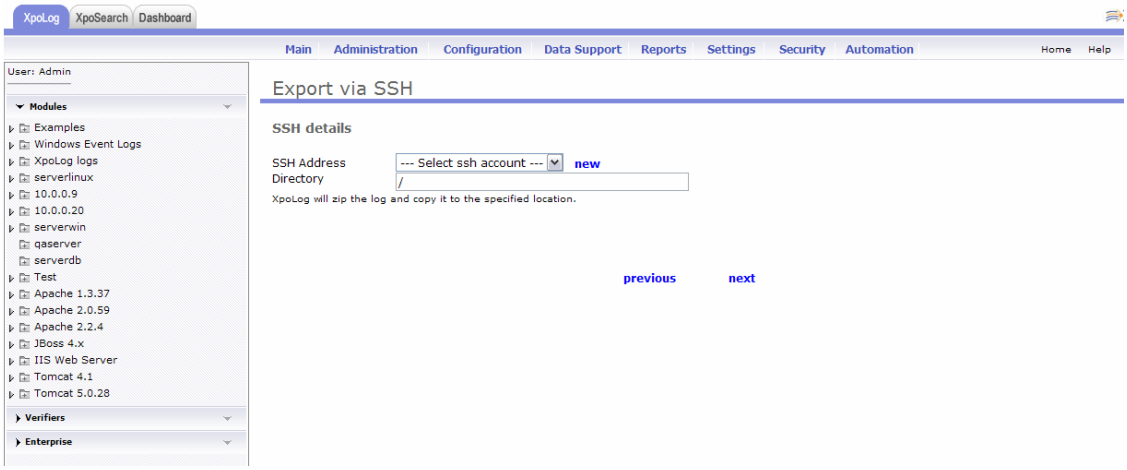
Click 'next' to start the transfer process.

Zip and copy to remote machine over SSH

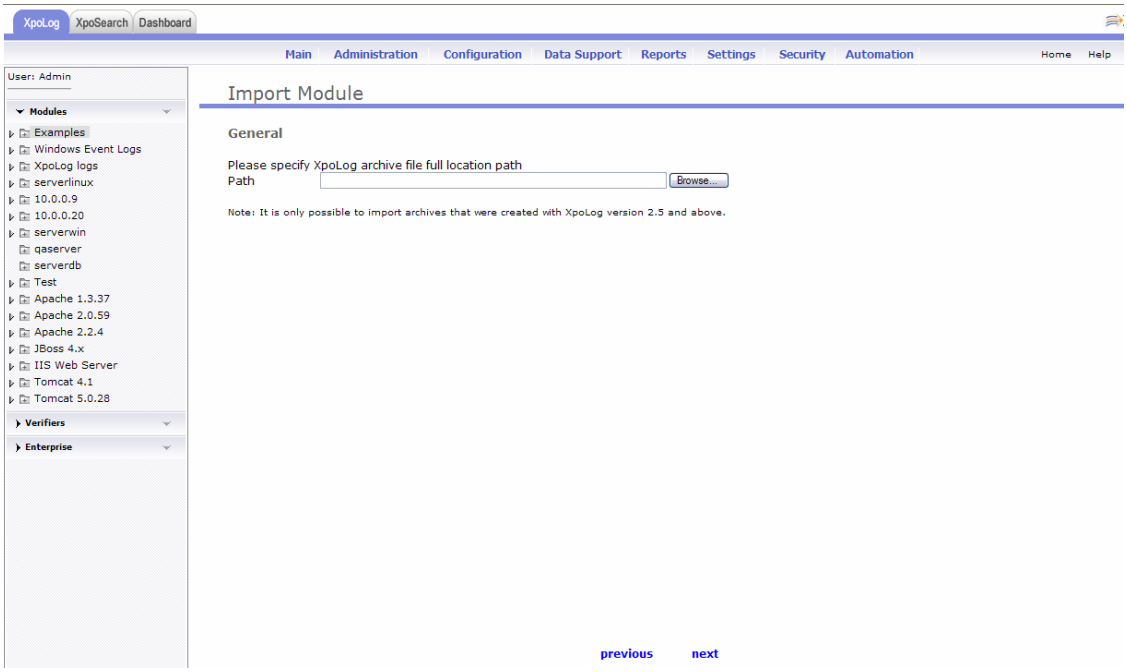
The module will be transferred over SSH to a remote machine. Select an SSH account from the list of available SSH accounts, or click new in order to configure a new SSH account. For further information regarding SSH accounts, please refer to Data Support → Address book.

Specify the directory on the remote machine, in which XpoLog will copy the module to.

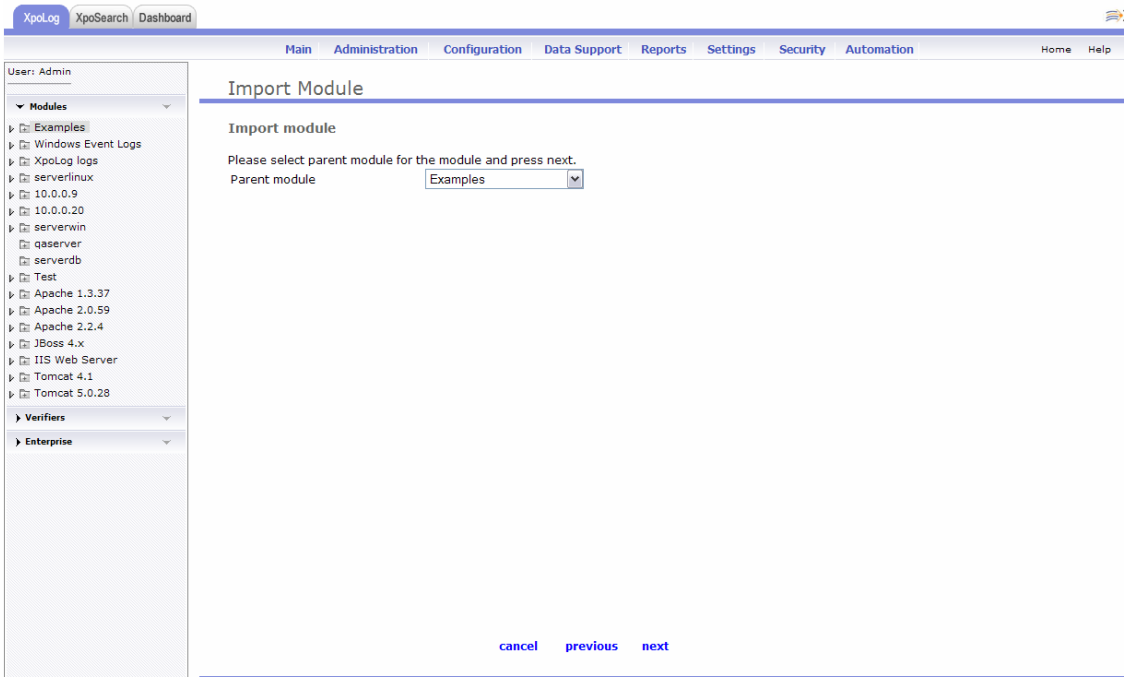
Click 'next' to start the transfer over SSH process.



Import module



In order to import a module to XpoLog, select ‘Import module’ from the data support menu. Specify the module’s path, and click ‘Next’



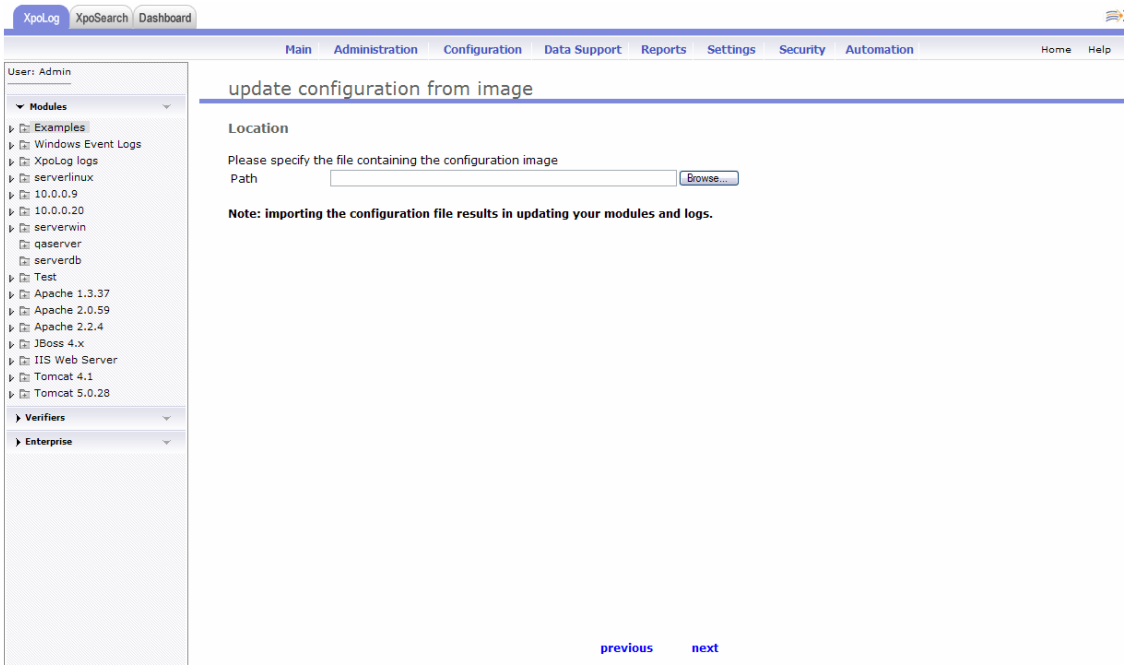
After locating the desired module, please select a parent module from the list of available modules. Click ‘next’ to finish the import process or ‘previous’ in case you would like to import a different module. Click ‘Ok’ to confirm the successful import.

Import configuration image

Importing a configuration image will update a vast part of XpoLog’s components, according to the specific saved image.

In order to import a configuration image, select ‘Import configuration image’ from the Data support menu.

For further information on how to save a configuration image, please refer to Configuration → Configuration image.

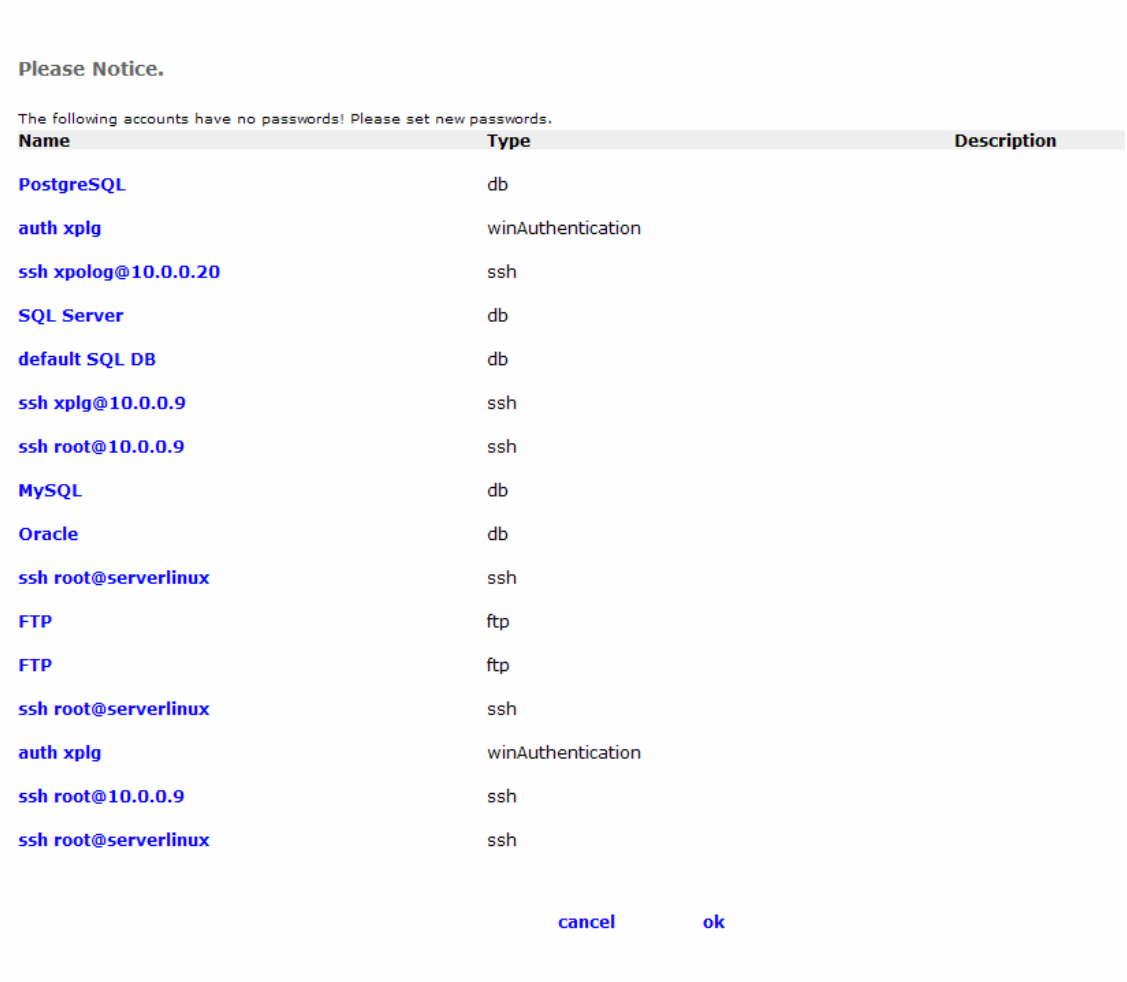


Specify the path where the saved image is located, and click ‘Next’.

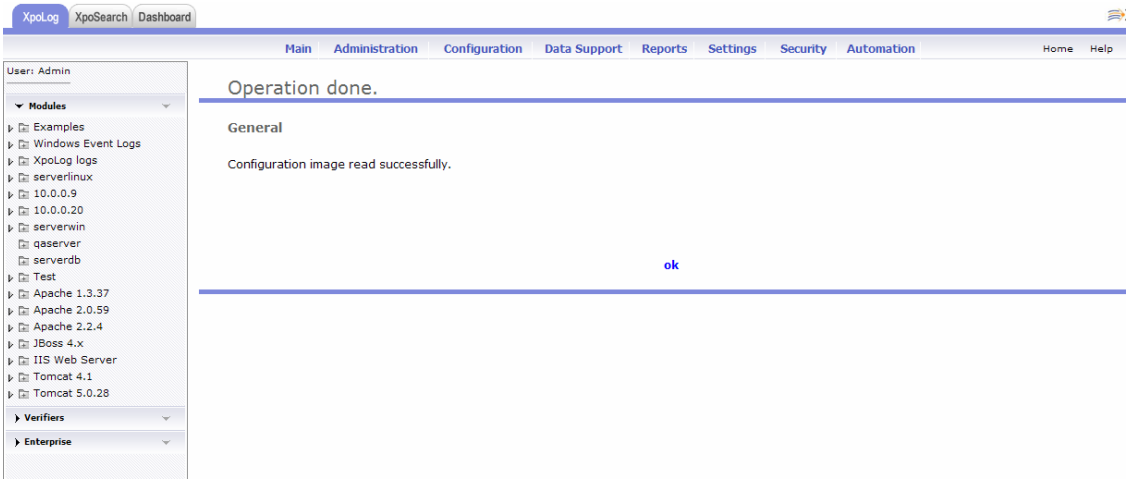
While XpoLog is importing the configuration image, a message will be displayed,

indicating that the import process might take a few minutes.

When XpoLog finished importing the configuration image, all accounts from the image that has no password will be displayed. Click each account name, and specify its password in order to be able to use it in XpoLog. Saving the account’s properties will lead you back to the import image wizard. When done setting passwords to all accounts, click ‘OK’ in order to finish the import image process.

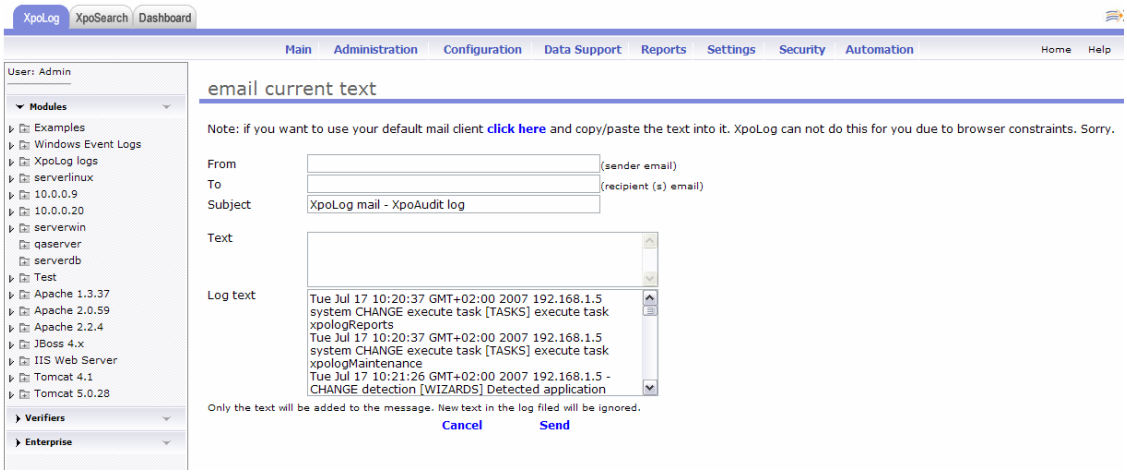


A message indicating that the new configuration image was successfully imported will be displayed. Click ‘OK’ to finish the import wizard.



Email text

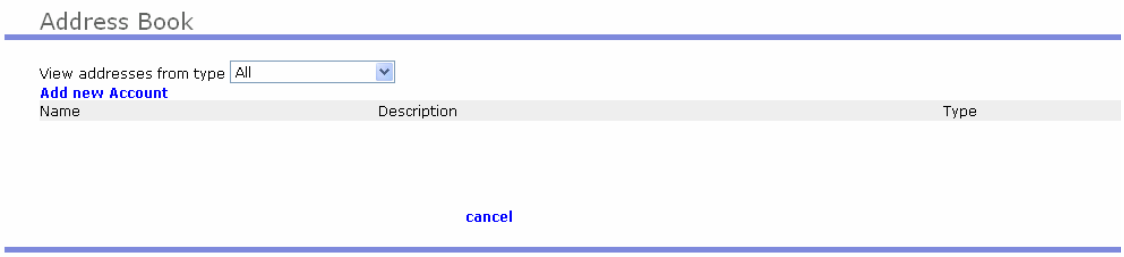
XpoLog allows you to send a log's content by email. While the specific log is in focus (In



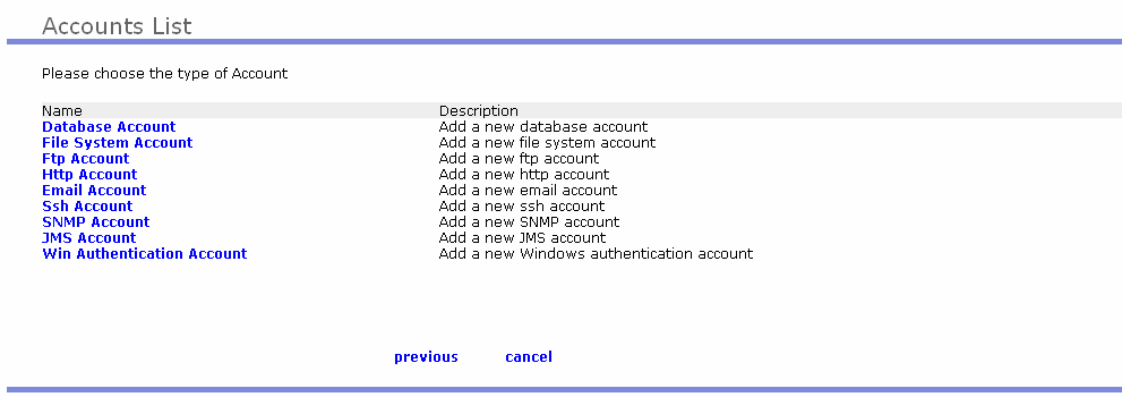
the log viewer) select the 'Email text' option from the Data Support menu.

Specify the sender's and recipient email. The default subject would be 'XpoLog mail – the name of the log', but you may change it, and add a text to the email as well.
Click 'Send' when done, or cancel to discard the email.

Address book

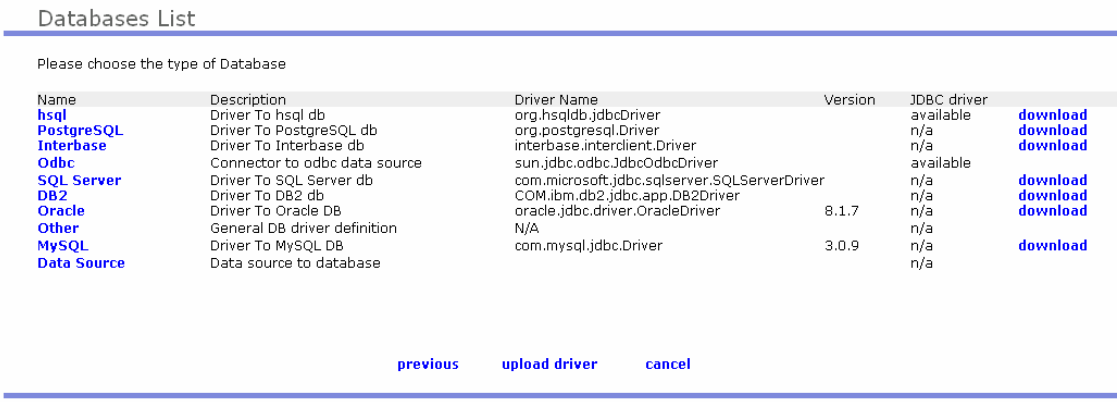


In order to create new accounts click the ‘Add new Account’ link.



Database Account

1. Click the ‘Database Account’ link from the ‘Accounts List’ page.



2. Choose the database type and specify the following configuration details (not all fields apply to all database types):
    - **Name:** the name of the new account.
    - **Description (optional):** the description of the new account.
    - **Driver Name:** filled in automatically.

- **User Name:** the username used to connect to the database.
- **Password (optional):** the password used to connect to the database.
- **Database Name:** the name of the database to connect to.
- **Machine Address:** the address of the machine on which the database is installed.
- **Port:** the port on which the database accepts connections.
- **Connection string params (optional):** parameters that should be passed upon connection.

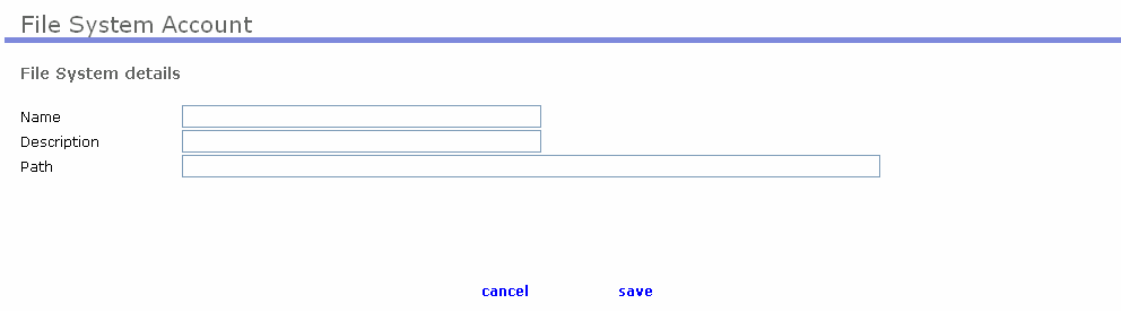
If you choose to add a Data Source (and not define a database account), you should specify the following configuration details:

- **Name:** the name of the data source.
- **Description (optional):** the description of the data source.
- **JNDI Name:** the JNDI name of the data source.
- **Environment Properties (optional)**
- **Database Type:** select the type of database the data source will work against (choose 'other' for an unknown database).

3. Click 'save' to save the new account.

File System Account

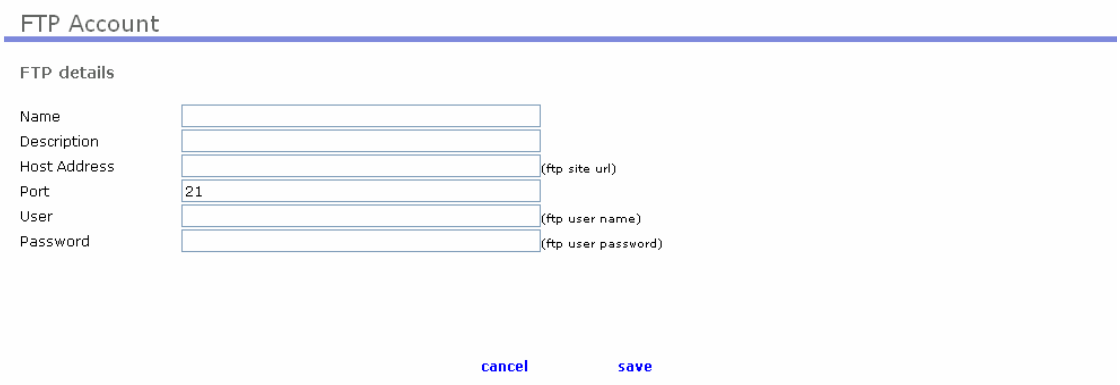
1. Click the 'File System Account' link from the 'Accounts List' page.



2. Specify the following configuration details:
   - **Name:** the name of the new account.
   - **Description (optional):** the description of the new account.
   - **Path:** the path in the file system the account points to.
3. Click 'save' to save the new account.

FTP Account

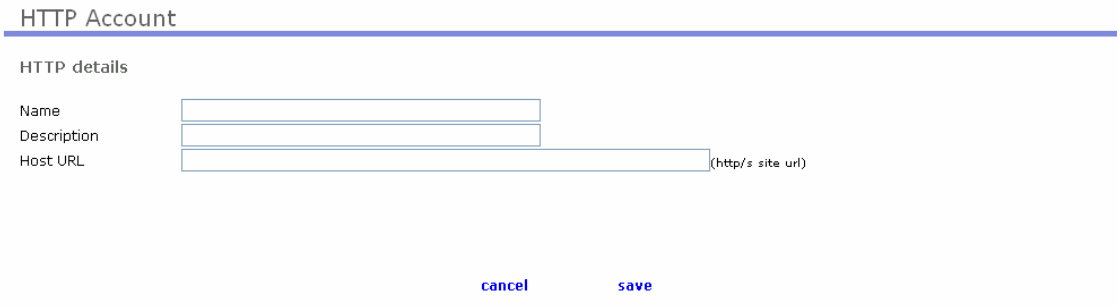
1. Click the ‘Ftp Account’ link from the ‘Accounts List’ page.



2. Specify the following configuration details:
    - **Name:** the name of the new account.
    - **Description (optional):** the description of the new account.
    - **Host Address:** the host name/IP address of the FTP site.
    - **Port:** the port on which the FTP server accepts connections.
    - **User:** the username used to connect to the FTP server.
    - **Password:** the password used to connect to the FTP server.
3. Click ‘save’ to save the new account.

HTTP Account

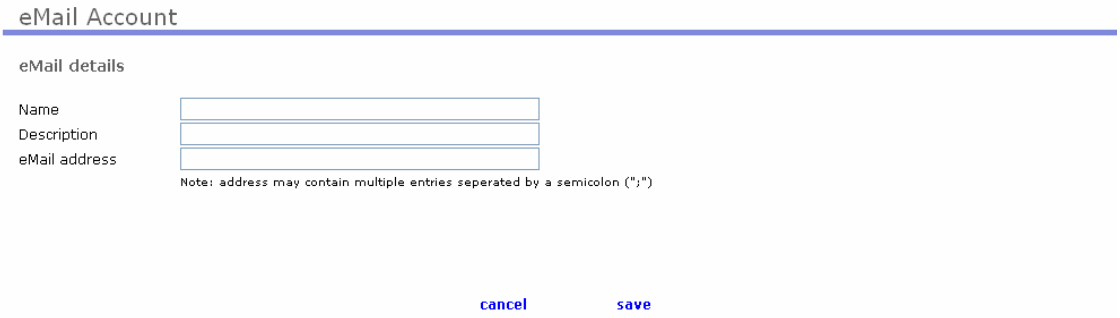
1. Click the ‘Http Account’ link from the ‘Accounts List’ page.



2. Specify the following configuration details:
    - **Name:** the name of the new account.
    - **Description (optional):** the description of the new account.
    - **Host URL:** the URL the account points to.
3. Click ‘save’ to save the new account.

Email Account

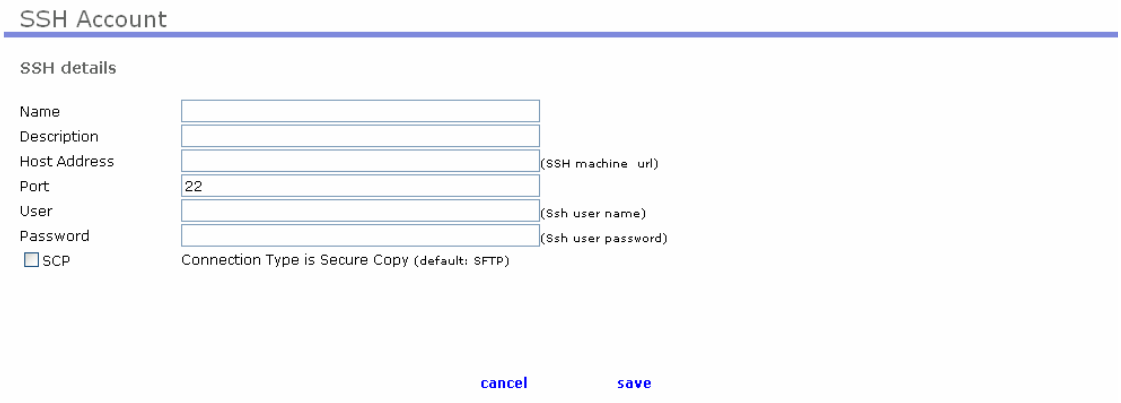
1. Click the ‘Email Account’ link from the ‘Accounts List’ page.



2. Specify the following configuration details:
    - **Name:** the name of the new account.
    - **Description (optional):** the description of the new account.
    - **eMail address:** the email address to be used by the account.
3. Click ‘save’ to save the new account.

Ssh Account

1. Click the ‘Ssh Account’ link from the ‘Accounts List’ page.



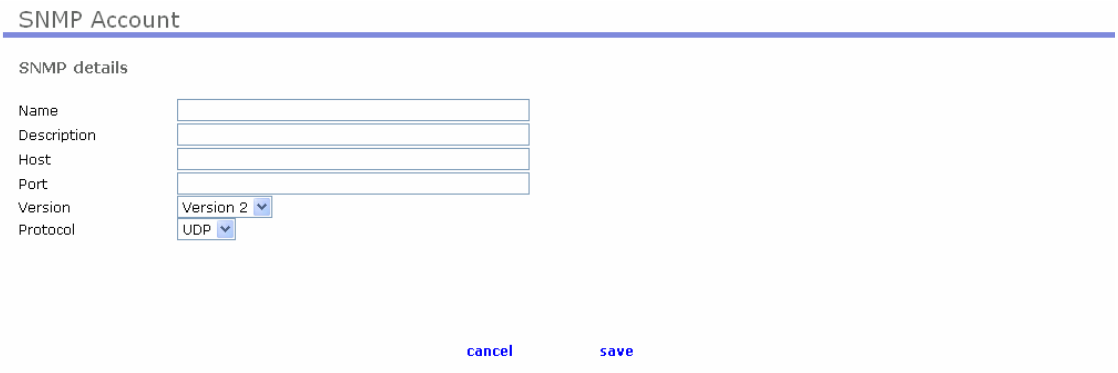
2. Specify the following configuration details:
    - **Name:** the name of the new account.
    - **Description (optional):** the description of the new account.
    - **Host Address:** the host name/IP address of the remote host.
    - **Port:** the port on which the remote host accepts SSH connections.
    - **User:** the username to be used to connect to the remote host.

- **Password:** the password to be used to connect to the remote host.
- **SCP:** check if the remote host does not support SFTP for file transfer.

3. Click ‘save’ to save the new account.

SNMP Account

1. Click the ‘SNMP Account’ link from the ‘Accounts List’ page.



2. Specify the following configuration details:
   - **Name:** the name of the new account.
   - **Description (optional):** the description of the new account.
   - **Host:** the host name/IP address of the remote host.
   - **Port:** the port on which the remote host accepts SNMP traps.
   - **Version:** the version of SNMP to be used.
   - **Protocol:** the protocol to be used.
3. Click ‘save’ to save the new account.

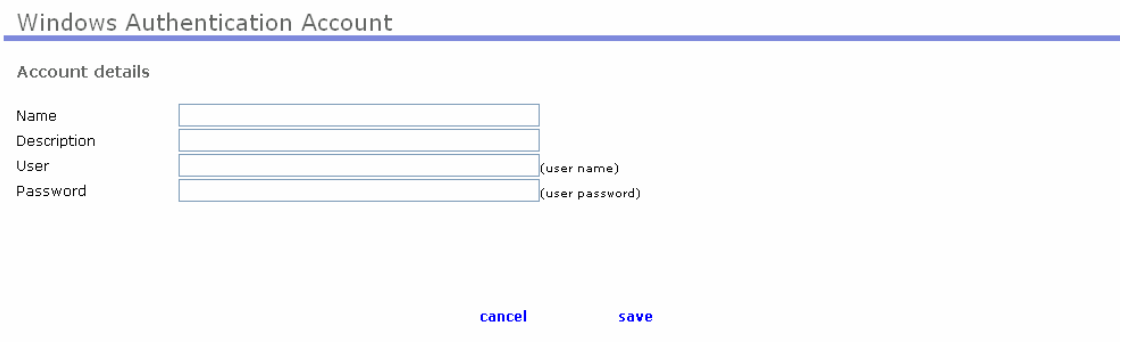
JMS Account

1. Click the ‘JMS Account’ link from the ‘Accounts List’ page.

2. Specify the following configuration details:
    - **Name:** the name of the new account.
    - **Description (optional):** the description of the new account.
    - **JNDI Context:** the full JNDI context.
    - **JNDI Provider URL:** the URL to be used to access the JNDI provider.
    - **User Name:** the username to be used to connect to the JNDI provider.
    - **Password:** the password to be used to connect to the JNDI provider.
    - **JMS Topic Factory:** the JNDI name of the JMS topic factory.
    - **JMS Queue Factory:** the JNDI name of the JMS queue factory.
3. Click ‘save’ to save the new account.

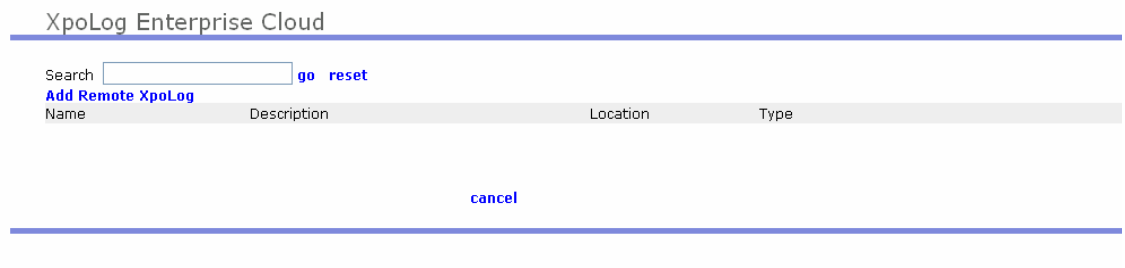
Win Authentication Account

1. Click the ‘Win Authentication Account’ link from the ‘Accounts List’ page.

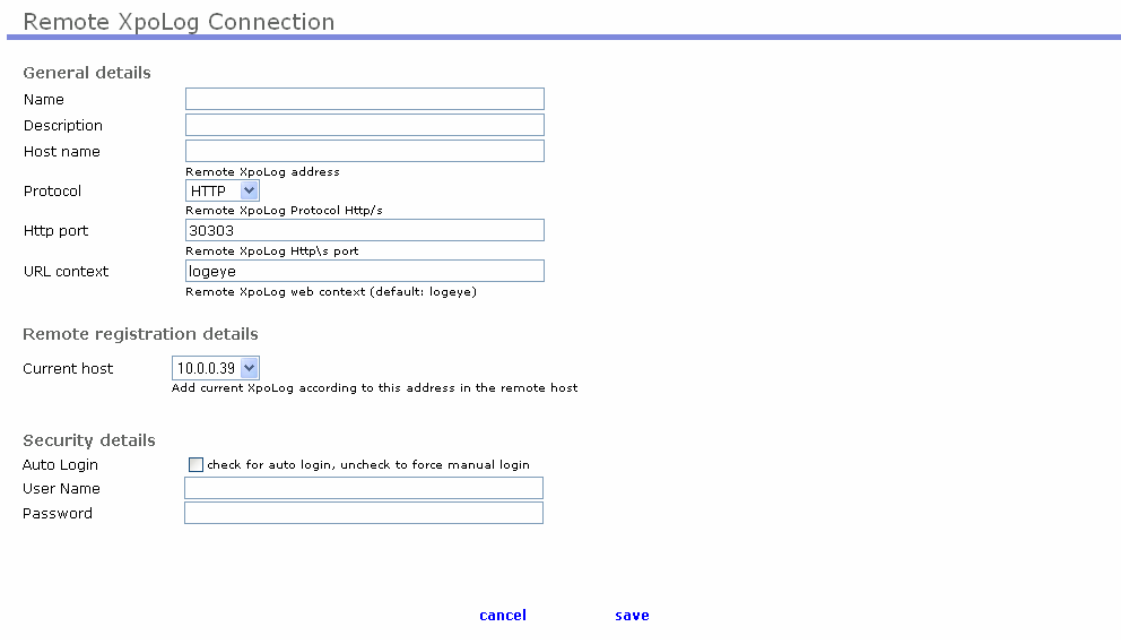


2. Specify the following configuration details:
    - **Name:** the name of the new account.
    - **Description (optional):** the description of the new account.
    - **User:** the username of the Windows Authentication account.
    - **Password:** the password of the Windows Authentication account.
3. Click ‘save’ to save the new account.

Enterprise



In order to create new remote XpoLogs click the ‘Add Remote XpoLog’ link.



Specify the following configuration details:

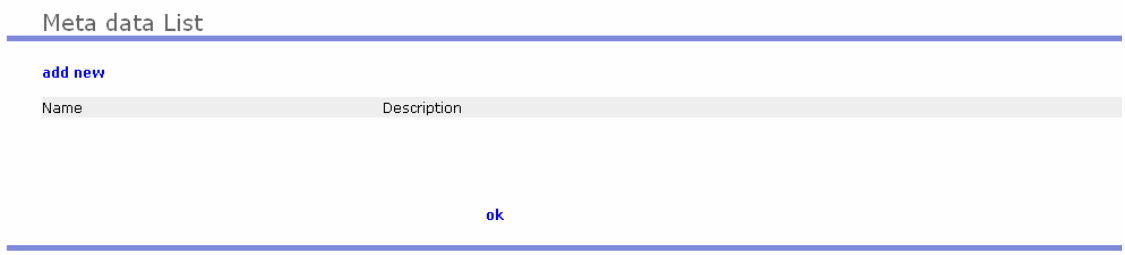
1. **General details**
   - **Name:** the name of the remote XpoLog.
   - **Description (optional):** the description of the remote XpoLog.
   - **Host name:** the host name/IP address the remote XpoLog is running on/
   - **Protocol:** the protocol allowed by the remote XpoLog.
   - **Http port:** the port on which the remote XpoLog is listening.
   - **URL context:** the context of the remote XpoLog.
2. **Remote registration details**
   - **Current host:** the host name/IP address to be used for the XpoLog node representing the current host that will be added in the remote XpoLog.
3. **Security details**

- **Auto Login:** when checked, no prompt for username and password will appear when accessing the remote XpoLog.
- **User Name:** the username to be used to access the remote XpoLog.
- **Password:** the password to be used to access the remote XpoLog.

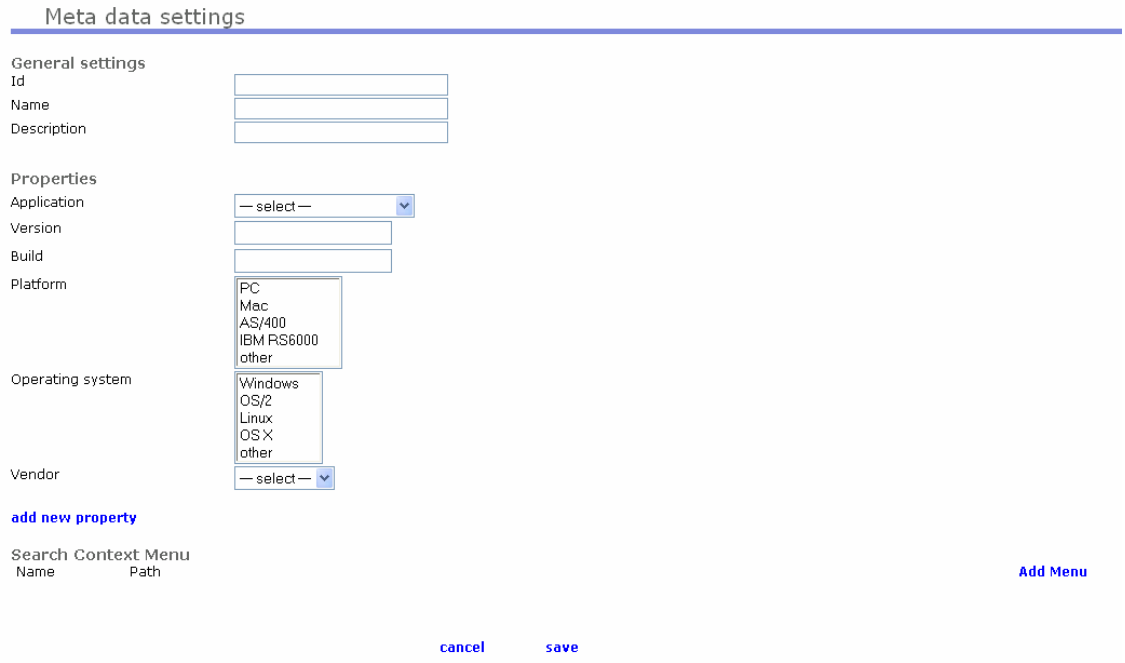
4. Click the ‘save’ link to save the new remote XpoLog.

After a remote XpoLog was added you can click its name to access it.
You can search remote XpoLog nodes by entering a search term in the ‘Search’ text box and clicking the ‘go’ link. Clicking the ‘reset’ link will display all remote XpoLogs that were added to the system.

Meta Data



In order to create new metadatas click the ‘add new’ link.



Specify the following details:

1. **General settings**
   - **Id:** the id of the new metadata.
   - **Name:** the name of the new metadata.
   - **Description (optional):** the description of the new metadata.
2. **Properties**
   - **Application (optional):** the application type of the new metadata.
   - **Version (optional):** the application version of the new metadata.
   - **Build (optional):** the application build of the new metadata.
   - **Platform (optional):** the platform of the new metadata. Choose other to specify a custom platform.

- **Operating system (optional):** the operating system of the new metadata. Choose other to specify a custom operating system.
- **Vendor (optional):** the vendor of the new metadata.

Click the ‘add new property’ link to add custom properties. Specify the type and value of each custom property.

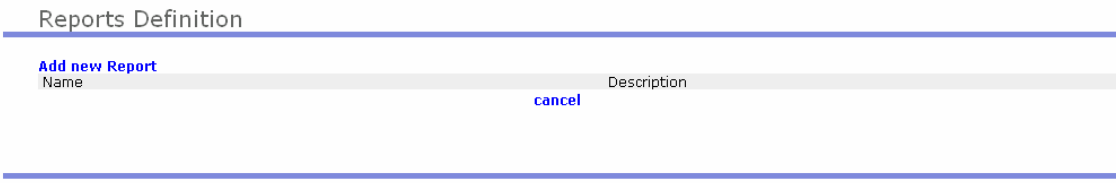
3. **Search Context Menu**

   Click the ‘Add Menu’ link to add custom search context menus. Specify the name and path of each custom menu.

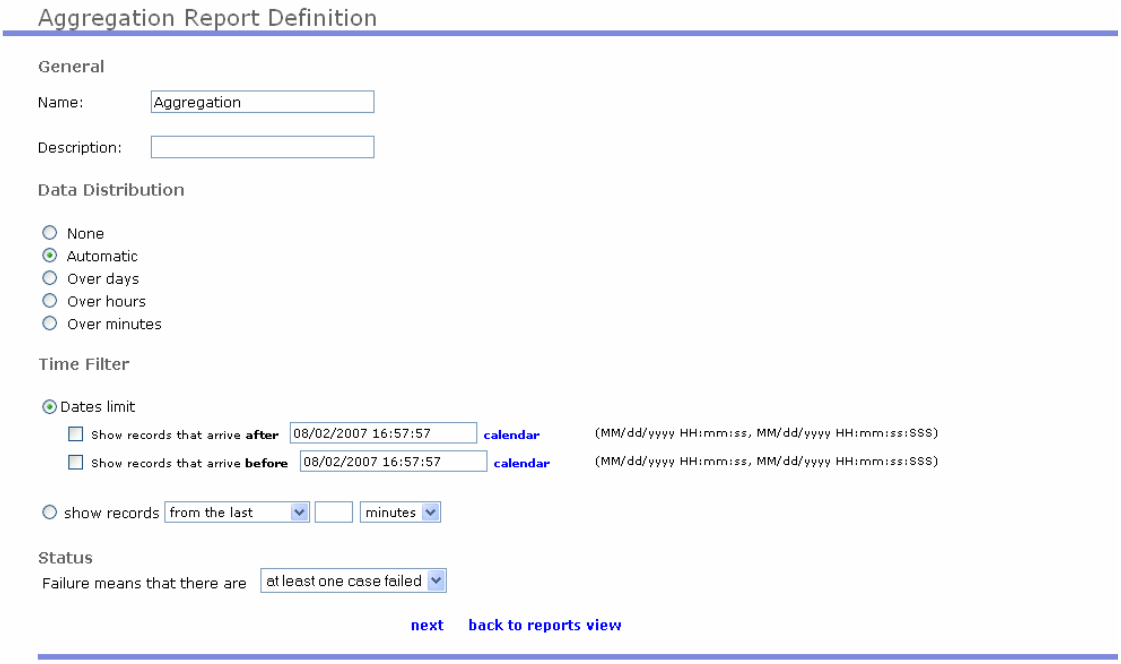
Click the ‘save’ link to save the new metadata.

Reports

Report Definition



This page shows all the reports in the system, grouped by the applications (metadata) they belong to. Reports that are not associated with any application are all grouped under 'Other'. Click the arrow next to an application to display its reports.
In order to add a new report definition click the 'Add new Report' link in the 'Reports Definition' page. After clicking the link the following page will appear:



1. **General**

   Enter the new report's name and description.

2. **Data Distribution**

   Select the data unit for which aggregation data will be computed (you can override this setting when you generate a new report runtime):

   - None: no computation of data distribution will take place. an empty cases distribution graph will be displayed

- Automatic: XpoLog sets automatically the data units either to ‘hours’ or ‘days’, according to the time span of the different data sources
- Over days: data will be aggregated for each day
- Over hours: data will be aggregated for each hour
- Over minutes: data will be aggregated for each minute

3. **Time Filter**

   Define default time constraints for the report generation (you can override this setting when you generate a new report runtime).

   You can define time constraints in two ways:

   - Selecting the ‘Dates limit’ option and entering the minimum and\or maximum date.
   - Selecting the ‘show records’ option. in the following combo box select one of the following options:
     - from the last: defines a time interval that starts with the specified time constraint and stretches until the current time
     - from the previous: defines a time interval that contains only the specified days, weeks or months
     - from: defines a time interval the starts in the data specified in number text field and time unit (in the case of ‘days’ a starting hour is required too) and stretches for the time span defined in the ‘for’ section of the filter

4. **Status**

   Select the logic by which the report’s status will be determined:

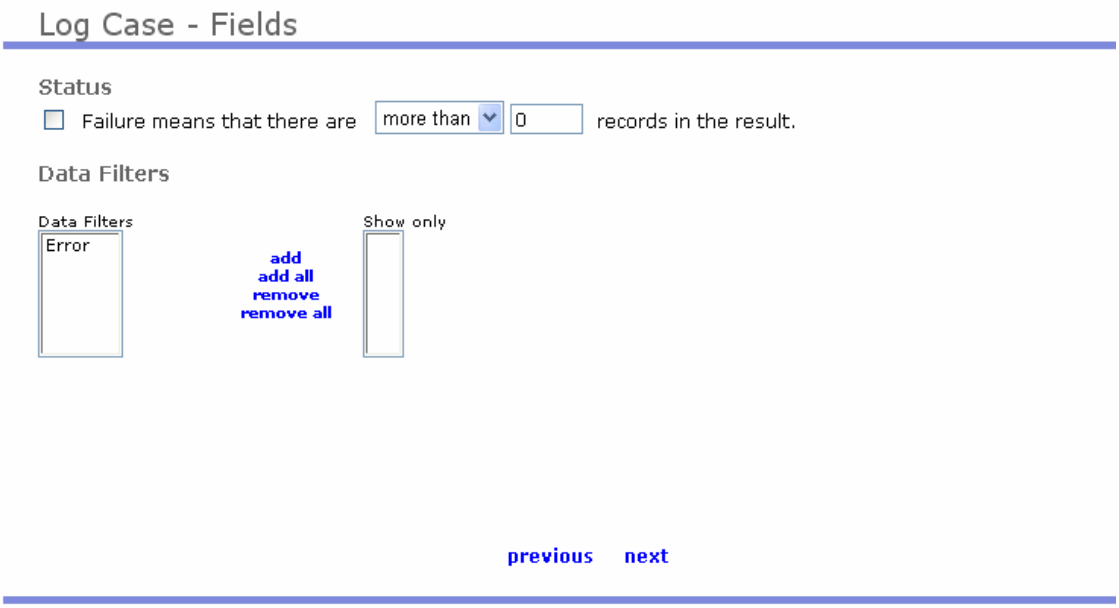
   - Select ‘at least one case failed’ in order to set the report status to ‘failed’ when at least one case/dimension has failed.
   - Select ‘all cases failed’ in order to set the report status to ‘failed’ when all of the report’s cases/dimensions have failed.

5. Click ‘next’ to continue to defining the report’s cases and dimensions (columns).

Define a new report case

1. Click ‘Add new aggregation rule’ to create a new case.

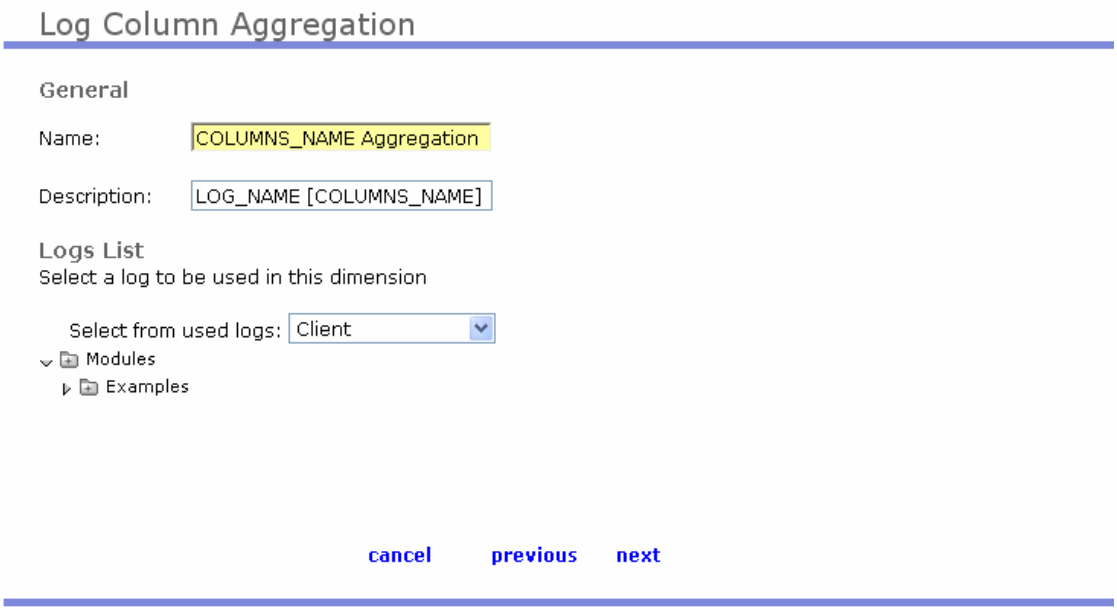
2. **General**
   - Enter the new case’s name and description. If you leave the default description ‘LOG_NAME [FILTERS_NAME]’, XpoLog will replace in the created report ‘LOG_NAME’ with the name of the selected log and ‘FILTERS_NAME’ with the name of the selected filter(s).
3. **Logs List**
   - Select the log to be used for the case. You can either select a log from the logs tree or select a previously selected log from the ‘Select from used logs’ combo box.
4. Click ‘next’ to continue to selecting filters to be included in the case.



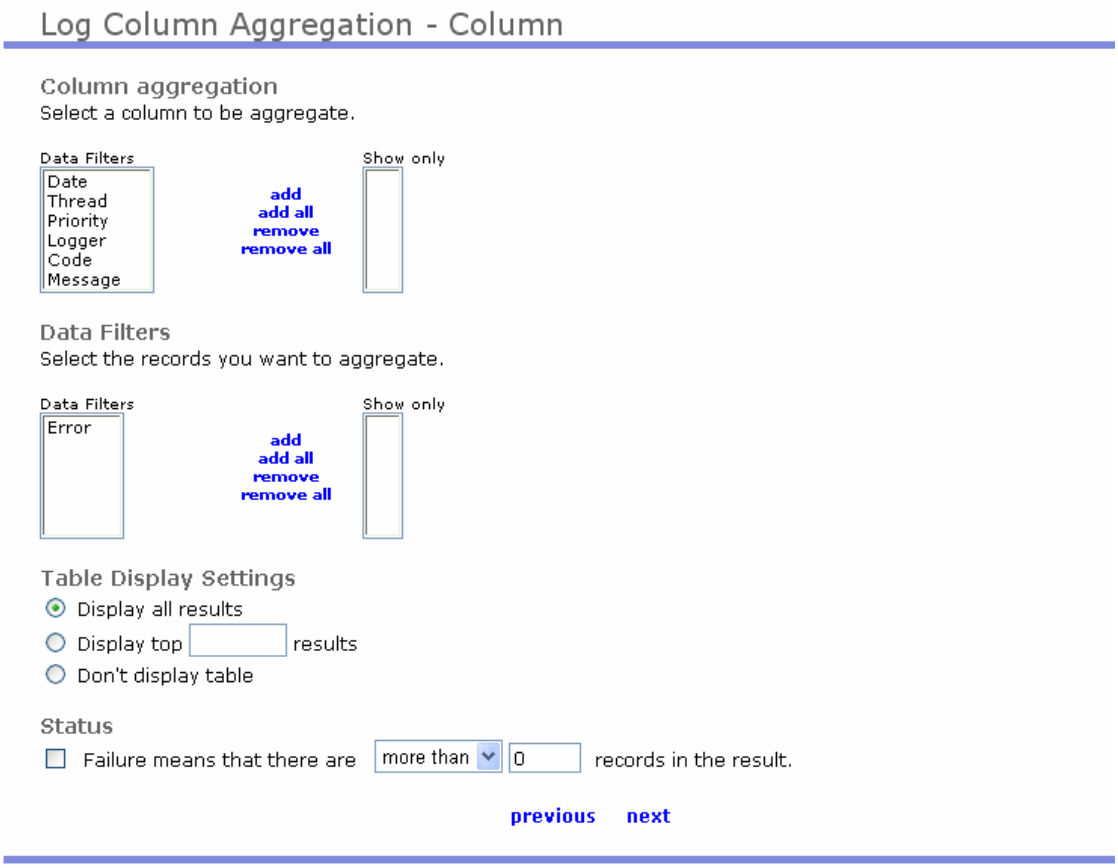
5. **Status**
    - Click on the check box to turn on the computation of the case's status. Select 'more than' or 'less than' and enter the number of records in the result to complete the definition of the case's status. If the checkbox is left unchecked, no status for that case will be computed.
6. **Data Filters**
    - Select the filters to be included in the case.
7. Click 'next' to continue adding the report's cases.
8. Repeat steps 1 to 7 to add more cases.
9. Click 'save' when finished adding the report's cases and dimensions.

Define a new report dimension (column)

1. Click ‘Add new column aggregation’ to create a new dimension.



2. **General**
   - Enter the new case’s name and description. If you leave the default name ‘COLUMNS_NAME Aggregation’ and description ‘LOG_NAME [COLUMNS_NAME]’, XpoLog will replace in the created report ‘LOG_NAME’ with the name of the selected log and ‘COLUMNS_NAME’ with the name of the selected column.
3. **Logs List**
   - Select the log to be used for the dimension. You can either select a log from the logs tree or select a previously selected log from the ‘Select from used logs’ combo box.
4. Click ‘next’ to continue to selecting columns and filters to be included in the dimension.



5. **Column aggregation**
    - Select the log's column to be aggregated.
6. **Data Filters**
    - Select the filters to be included in the dimension.
7. **Table Display Settings**
    - Set the number of results to be displayed in the column section of the report runtime result:
        - Select 'Display all results' to show all distinct values (XpoLog collects only the top 5000 distinct values).
        - Select 'Display to X results' and specify the number of distinct values to be displayed.
        - Select 'Don't display table' to display only a graph.
8. **Status**
    - Click on the check box to turn on the computation of the dimension's status. Select 'more than' or 'less than' and enter the number of records in the result to complete the definition of the dimension's

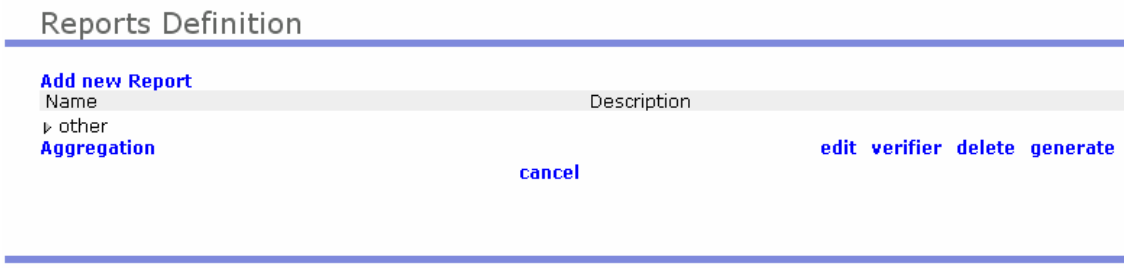
status. If the checkbox is left unchecked, no status for that dimension will be computed.

9. Click ‘next’ to continue adding the report’s dimensions.

10. Repeat steps 1 to 9 to add more dimensions.

11. Click ‘save’ when finished adding the report’s cases and dimensions.

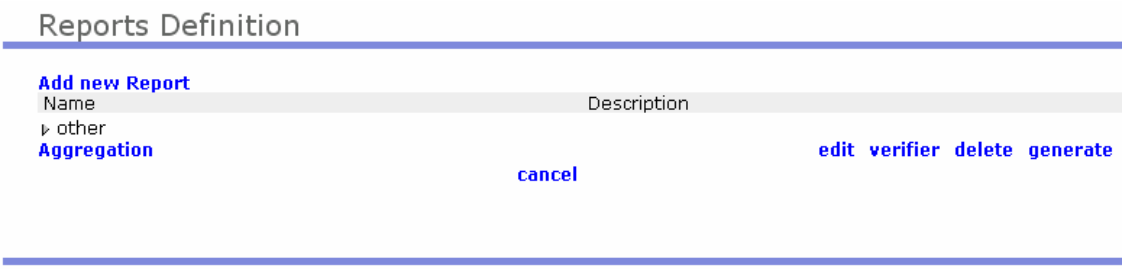
Report Generation



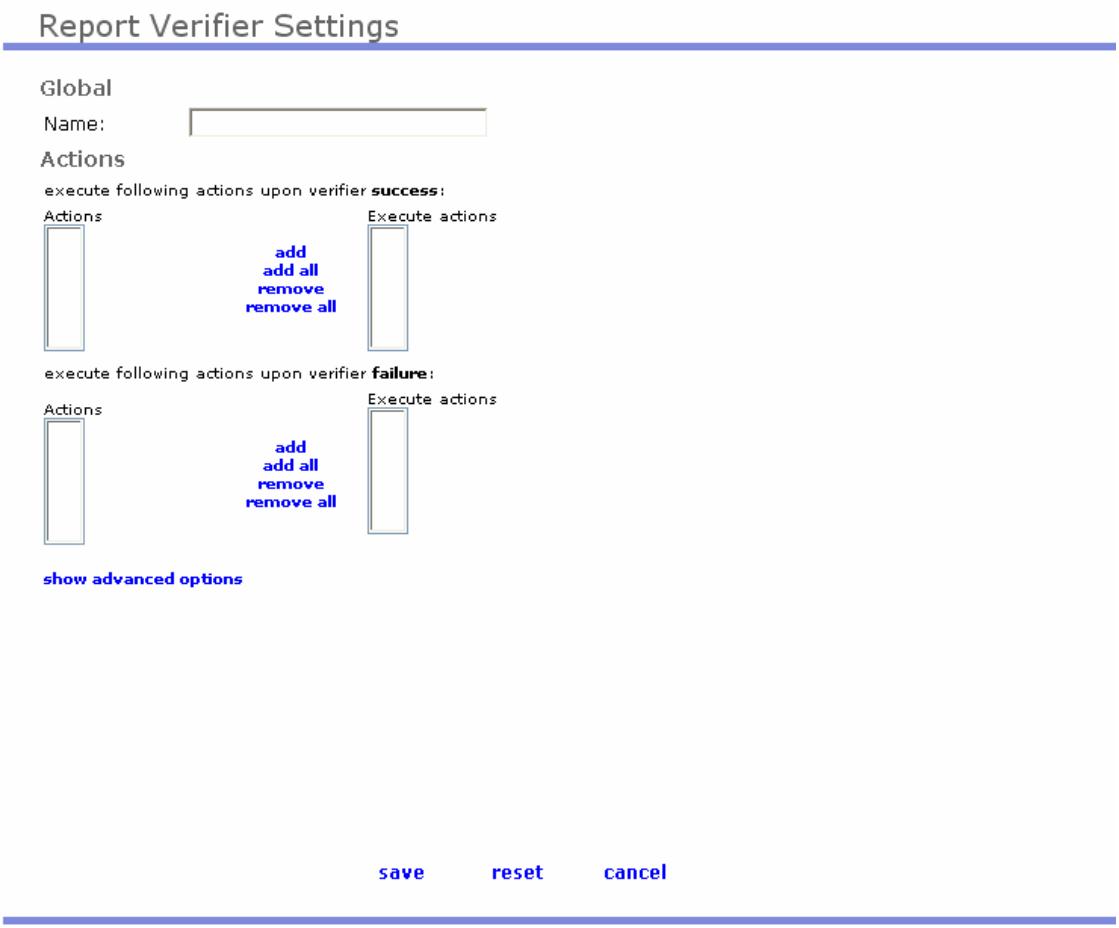
1. Click ‘generate’ or click the report name to enter the ‘Reports Runtime’ page and click the ‘Generate new report runtime’ link.

2. The ‘Data distribution’ and the ‘Time Filter’ are taken from the report definition. You can override these values for each report execution.
3. Click ‘generate’ to generate the report.

Report Verifier



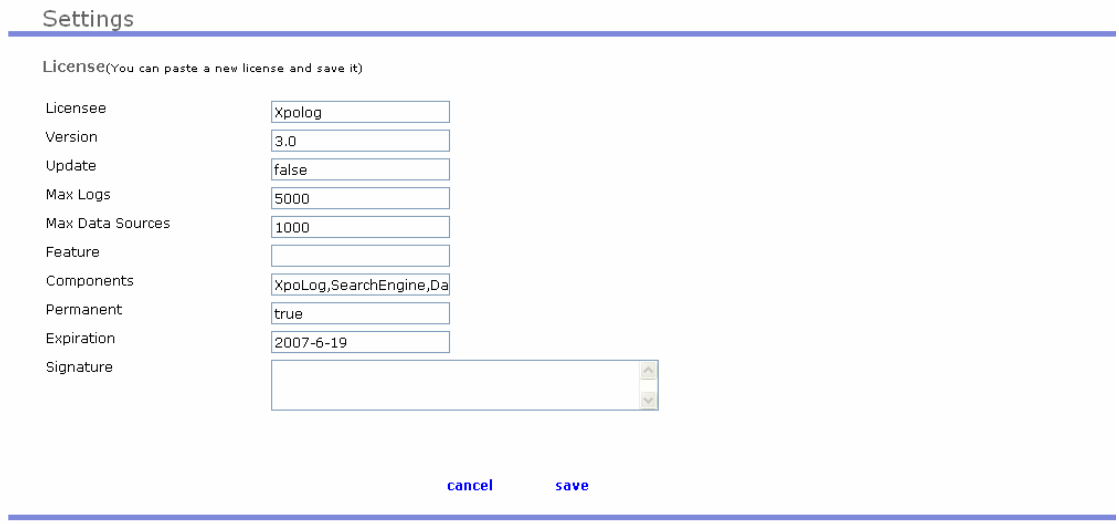
1. Click ‘verifier’.



2. **Global**
    - Enter the name of the report verifier.
    - Select the actions to take place upon verifier success and failure.
3. Click ‘save’ to save the verifier.

Settings Menu

License



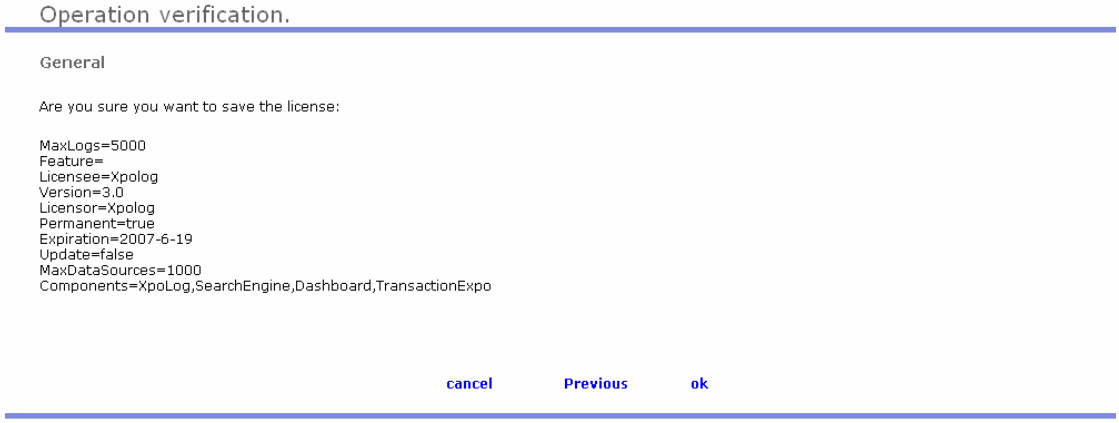
This page is used to update the license of XpoLog.

In order to update your license, execute the following steps:

Open the license.lic file that contains your license details.

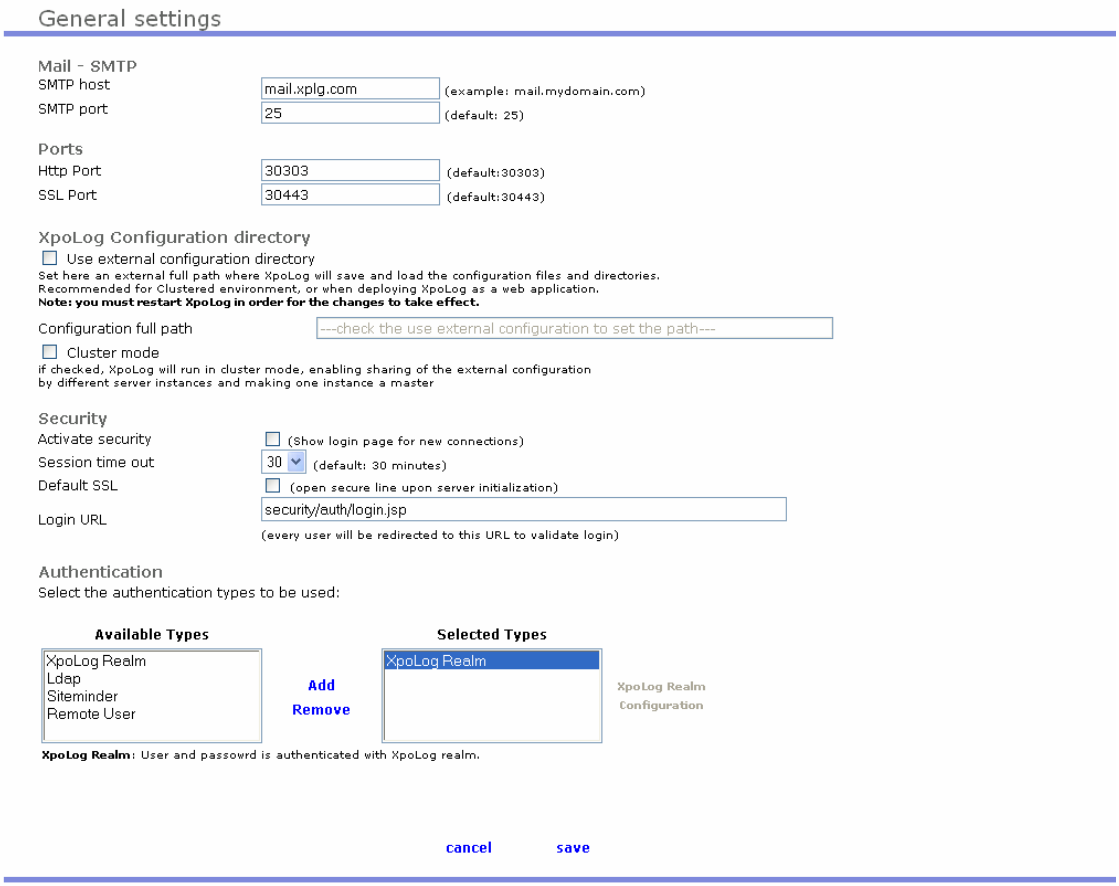
Paste the value of each filed in the appropriate location.

Click the ‘save’ link.



Verify the license details and click the ‘ok’ link to confirm.

Settings → General



This page is used to update XpoLog's general settings. When you are finished updating the settings click the 'save' link for the changes to take effect.

- **Mail - SMTP**

  Use this section to configure the SMTP host and port XpoLog should use to send emails.

- **Ports**

  Use this section to configure the HTTP and HTTPS ports XpoLog will be listening on.

- **External Configuration**

  you may save the entire configuration that XpoLog is using in a specific location. To do so, execute the following steps:

  1. Click the 'Use external configuration directory' check box.
  2. Specify the path in which you XpoLog's configuration to be saved in the 'Configuration full path' text box.

3. If you want XpoLog to run in cluster mode, check the ‘Cluster mode’ check box.

Note that changing this setting requires performing a restart of XpoLog.

- **Security**

  Use this section to configure XpoLog’s security settings. The following settings are available:

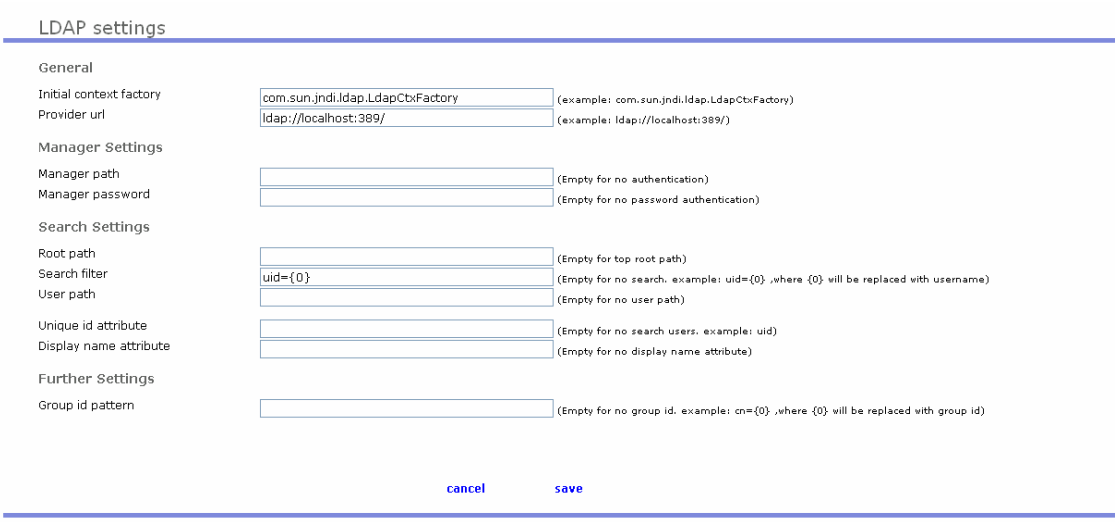
  1. Activate security - you can activate XpoLog’s security mechanism by clicking the ‘Activate security’ check box. **Note** that after activating the security mechanism and clicking the ‘save’ link you will be redirected to XpoLog’s login page, where you will be asked to enter a username and password to access XpoLog. In addition, a new menu, ‘Security’, will be added to XpoLog’s top menu.
  2. Session time out – use this setting to configure the session timeout period (in minutes). The default session timeout period is 30 minutes.
  3. Default SSL – use this setting to redirect XpoLog’s users to a secure channel (SSL) by default.
  4. Login URL – use this setting to configure the URL to which users will be redirected for login.

- **Authentication**

  Currently, XpoLog provides 4 different pre defined authentications types: XpoLog realm, Active Directory/LDAP, Siteminder and Remote user.
  Various different authentication methods have been successfully implemented in XpoLog over the past few years. In case your company uses a different authentication method then the one in the available types, please contact our support team for further assistance.
  Both the LDAP and the Siteminder authentication methods should be configured before use.

  <u>Active Directory/LDAP Configuration</u>:

  Select LDAP from the table on the left (‘Available types’), and add it to the ‘Selected types’ table. Click the ‘LDAP configuration’ link:



- General:

  Initial context factory – you may leave as default.

  Provider URL – set the connection URL to the LDAP server.

  Manager Settings (this is optional):

  Manager Path – the manager DN for searching users.

  Manager password – the manager's password.

  Search Settings:

  Root Path – the path for start searching users.

  Search Filter – how to search the users in the LDAP directory (the {0} is replaced with user name).

  User Path- full path of the user DN (the {0} is replaced with user name). For example: uid={0},ou=people,cn=xplg

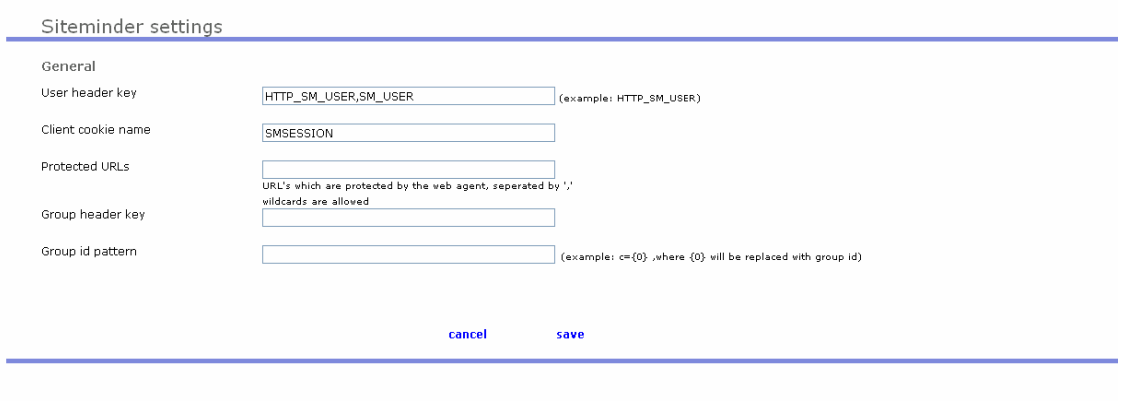
  Unique Id – optional, which attribute of the user will be provided as the unique id of the user.

  Display name attribute – optional, which attribute of the user will be provided as the display name of the user.

  Save the LDAP configuration, and save the general settings configuration.

  XpoLog will then authenticate users with the LDAP server.

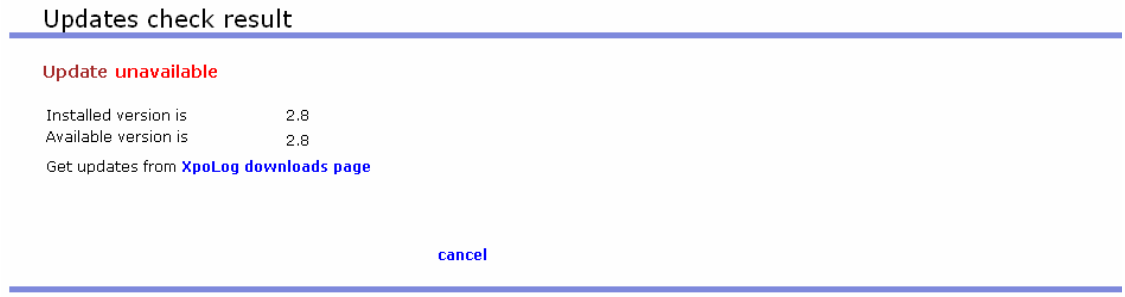
Siteminder Configuration:



- Click the Siteminder Configuration link in order to configure it:
  In order to set more header key for retrieving the user information which was authenticated, you may use ‘,’ as a separator between parameters. For Example: HTTP_SM_USER, HTTP_UID – in this case XpoLog will look for the user first in the HTTP_SM_USER header key, and then if not found in the HTTP_UID header key.
  You may use as many keys as you wish.

- Save the Siteminder configuration, and save the general settings configuration. XpoLog will then associate users in XpoLog according to Siteminder’s authentication.

Updates



This page is used to check if there is a newer version of XpoLog available for download from XpoLog's download page.

UI Settings

This page is used to change the look and feel of XpoLog. The available changes are:

CSS definition:

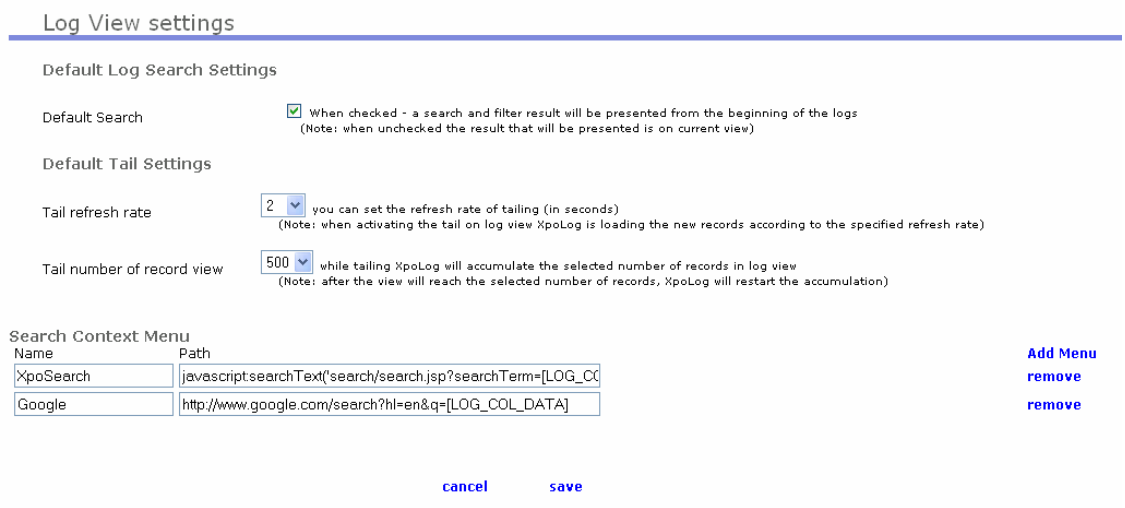
Click the 'Edit CSS File' to read an explanation on how the CSS files can be edited.

XpoLog's CSS files resides in XpoLogInstallationDir\defaultroot\logeye\css

Edit Images:

click the 'Edit Images' link to specify new paths for images you wish to replace.

Log View Settings



This page is used to update settings common to all log views. The available settings are:

- **Default Log Search Settings**

  checking the 'Default Search' check box will cause searches to be performed from the beginning of a log. Leaving it unchecked will cause searches to be performed from the current position.

- **Default Tail Settings**

  This section controls the configuration of the tail feature. The available settings are:

  - Tail refresh rate: specify the number of seconds between each tail refresh action. The default refresh rate is 2 seconds.
  - Tail number of record view: specify the number of records that will be accumulated in the log view before switching to a new page. The default number of records is 500.

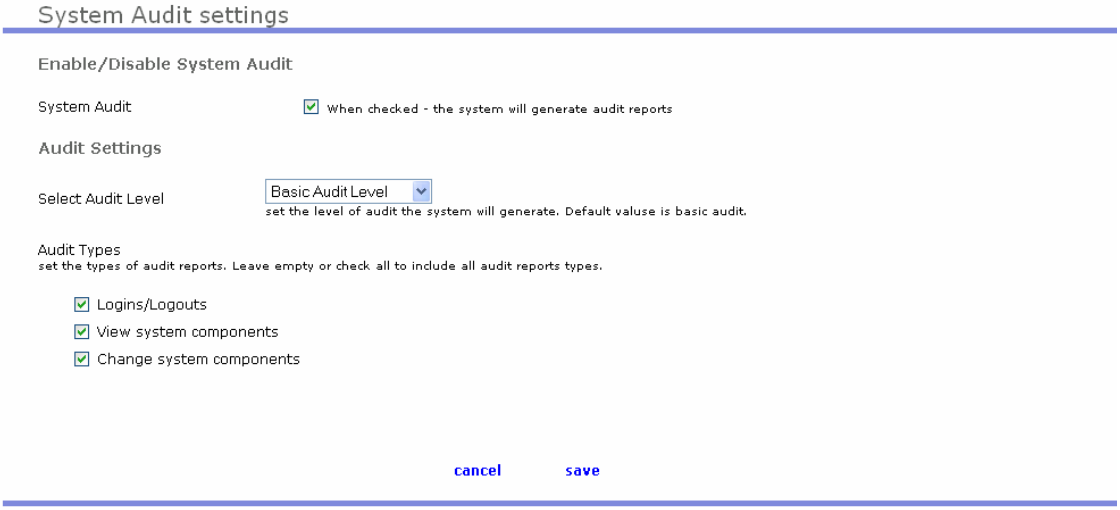
- **Search Context Menu**

  it is possible to define a search context menu to enable search of logged data in data repositories, such as search engines and wikis.

  Add a search context menu to all logs by specifying the name of the data repository (i.e. Google) and the URL to be used for the search.

  Note that the URL can contain place holders for dynamic text replacement during the search.

System Audit



This page is used to configure XpoLog's audit settings. The available settings are:

- **Enable/Disable System Audit**

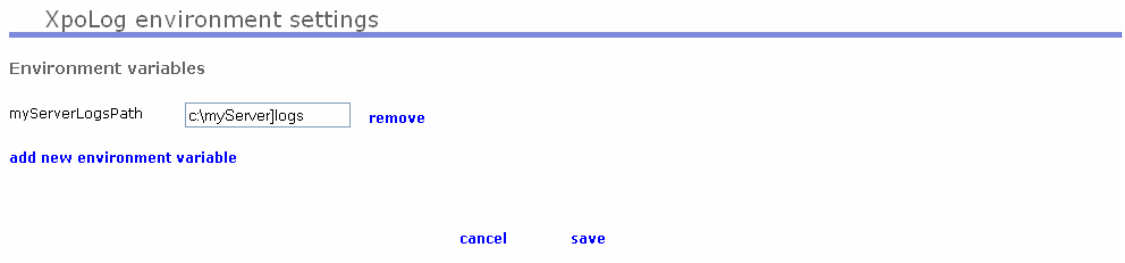
  Click the 'System Audit' check box to enable or disable system audit.

- **Audit Settings**

  Use the 'Select Audit Level' combo box to specify the level of audit you wish XpoLog to produce.

- **Audit Types**
  - Logins/Logouts: when checked, users' login and logout operations will be audited.
  - View system components: when checked, users' viewing operations will be audited.
  - Change system components: when checked, users' editing operations will be audited.

Environment Variables



This page is used to specify variables that can be user all across XpoLog. For example, you can add an environment variable that points to a logs folder, and in every log you add you only need to put the environment variable's name in the path, and not the full path. This way, if the path changes, you only need to edit the environment variable's value and all the logs will remain functional.

If the variable's name is **myServerLogsPath**, the value to be used in order to access it is ${**myServerLogsPath**}

Note that after adding, editing or removing environment variables you must click the 'save' link for the changes to take effect.

Audit

This page is used to generate a filtered log view on audited data. The available filters are:

- **Time Frames**

  specify the time frame of the audit view.
- **Audit Types**

  specify the types of actions you wish to view.
- **General**
  - User Name: specify a user whose audit you wish to view.
  - General: specify a general term to be included in the filter, such as component name or action description.

After you are finished specifying the filter criteria click the ‘generate’ link to open the filtered audit log view.

About

This page is used to view XpoLog's version and installed patches. The following actions are available:

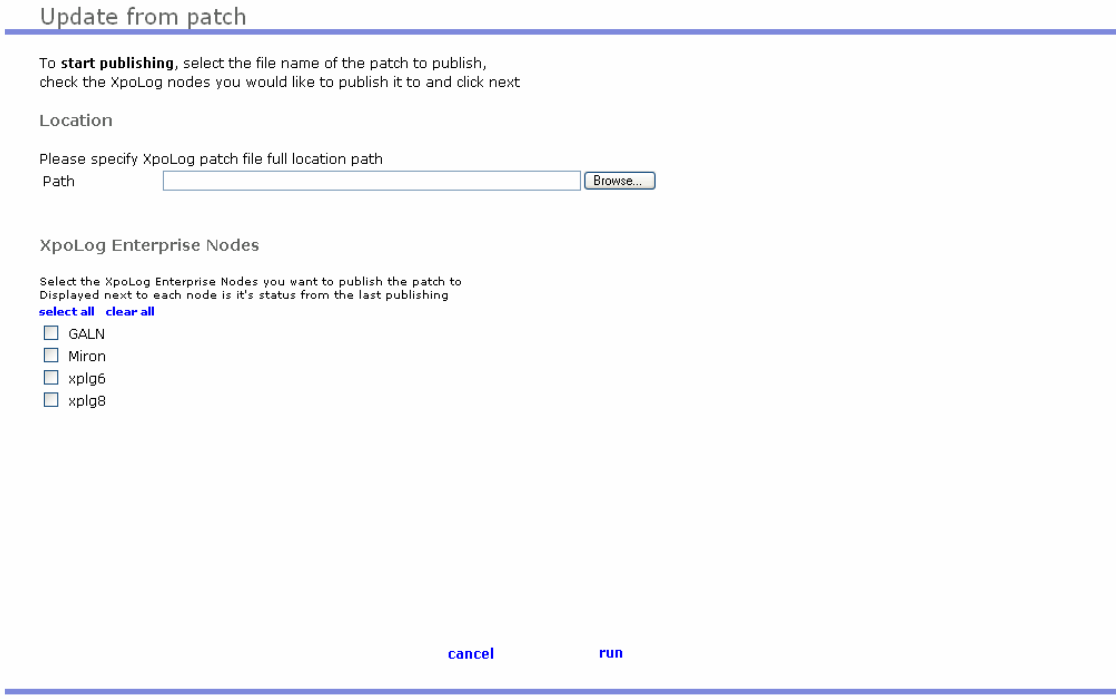
- **Add patch**

  click the 'add patch' link to add a patch to the system. The following page will appear:

  use the 'Browse' button to choose the patch and click the 'run' link to apply the patch.

- **Publish patch**

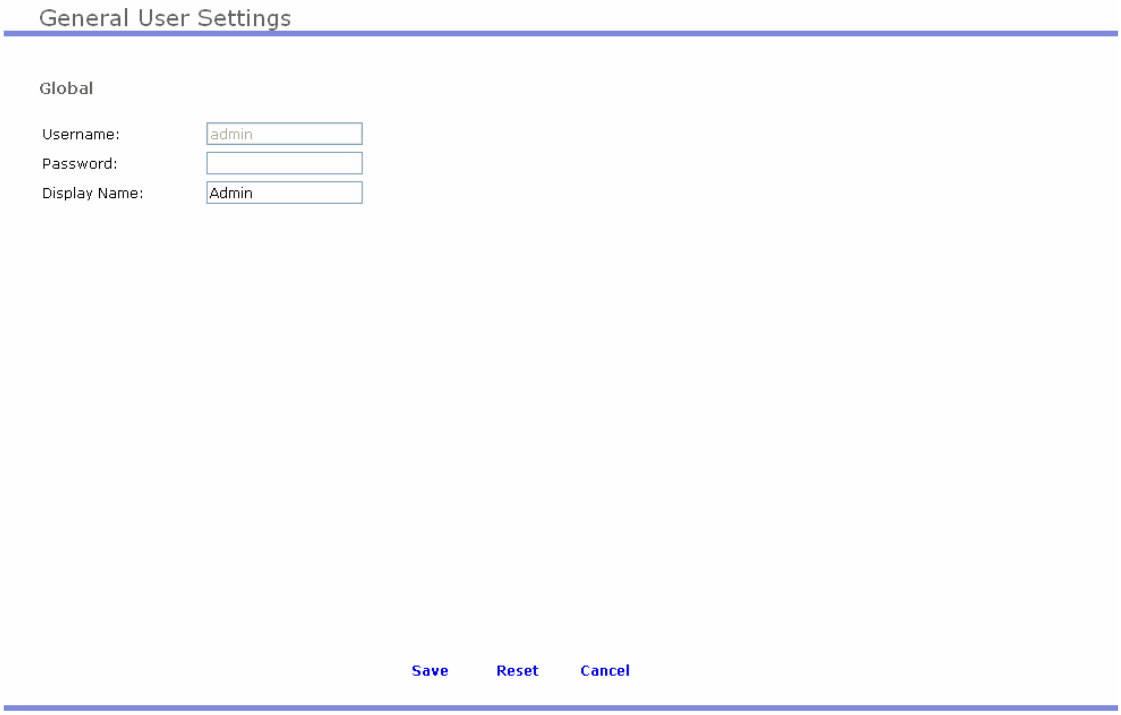
  click the ‘publish patch’ link to distribute a patch to other XpoLog nodes that exist in your enterprise. The following page will appear:



  use the ‘Browse’ button to choose the patch, choose the XpoLog nodes to which you want the patch to be published and click the ‘run’ link to publish the patch.

Security

User general settings



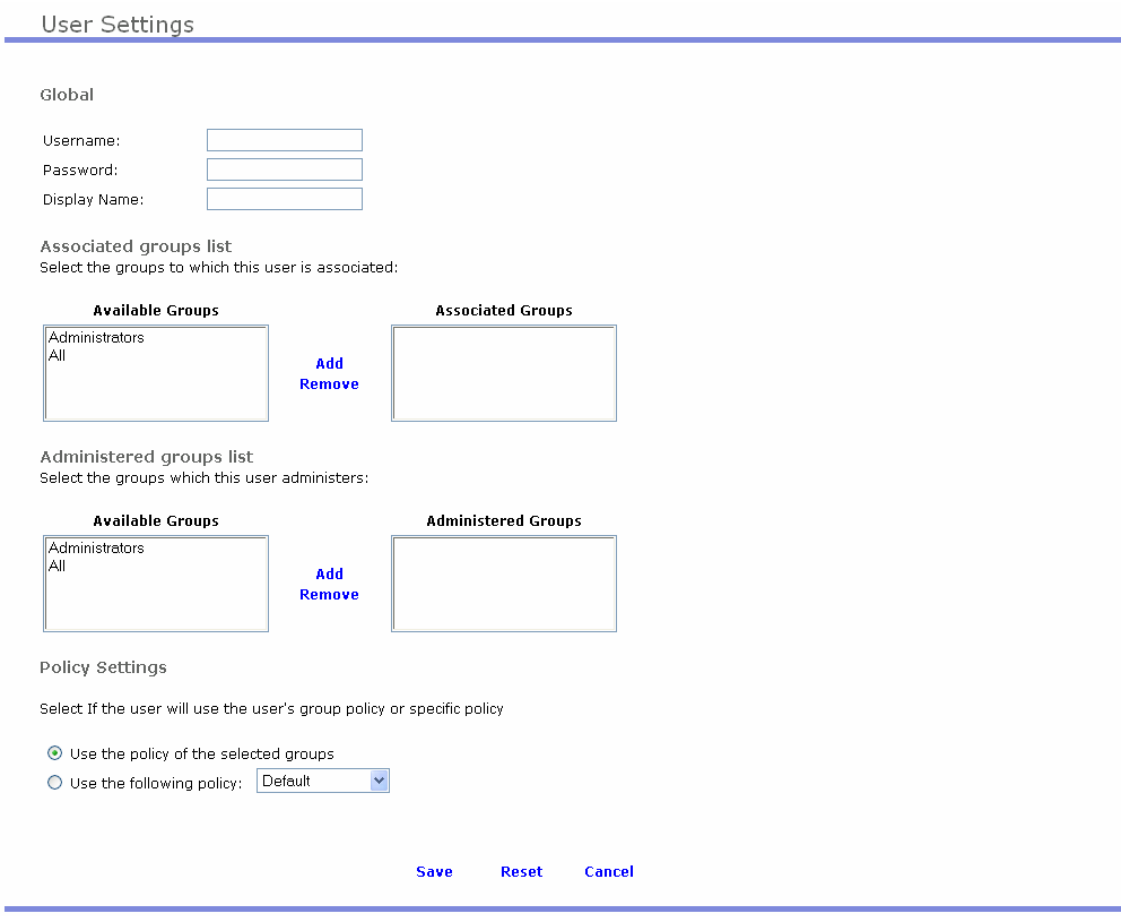
Use this page to change the password and display name of the current user.

Click the ‘Save’ link to apply the changes.

Users view

Use the ‘Groups’ combo box to filter the users view by groups.

Click the ‘Add User’ link to create a new user.



Specify the following details of the new user:

Global

- **Username:** the username identifying the new user.
- **Password:** the password of the new user.
- **Display Name:** the name that will be displayed across the system.

Associated groups list: select the groups to which the user is associated.

Administration groups list: select the groups which the user administers.

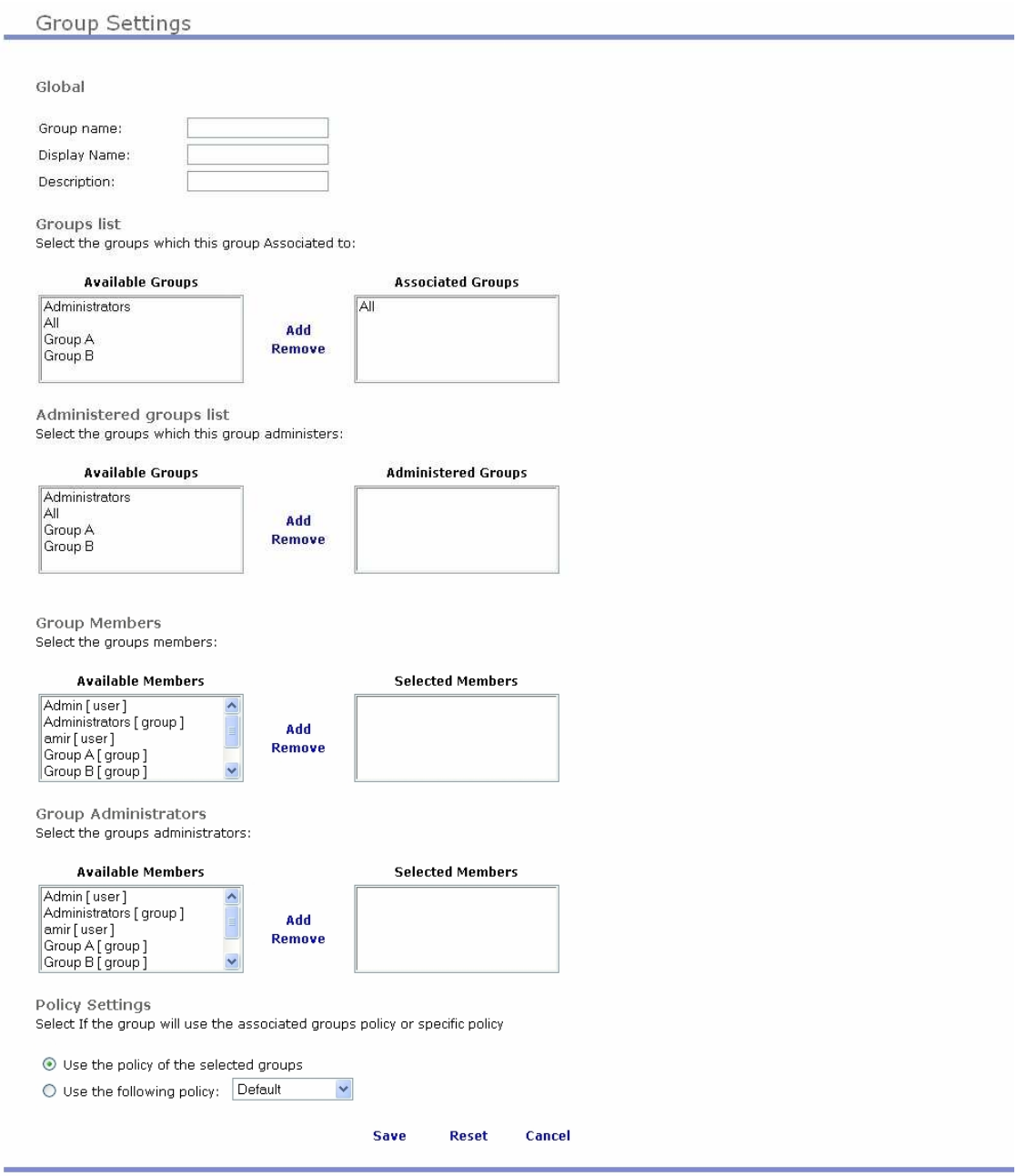
Policy Settings: specify the policy to be associated with the user. Select from using the policy of the groups to which the user is associated or select a specific policy.

Click the 'Save' link to save the new user definition.

Groups view

Use the ‘Groups’ combo box to filter the groups view by groups.

Click the ‘Add Group’ link to create a new group.



Specify the following details of the new group:

Global

- **Group name:** the name identifying the new group.
- **Display Name:** the name that will be displayed across the system.
- **Description (optional):** the description of the new group.

Groups List: select the groups which the group is associated to.

Administered Groups List: select the group which this group administers.

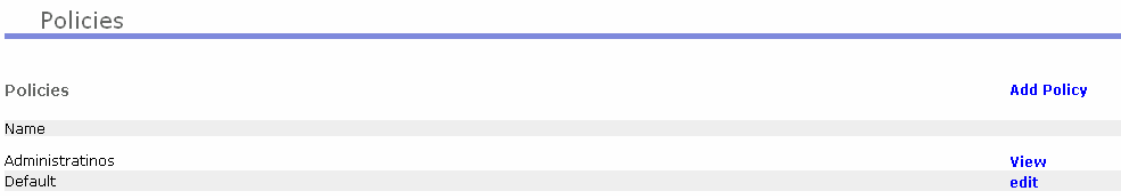
Group Members: select the users and groups that belong to the group.

Group Administrators: select the users and groups that administer the group.

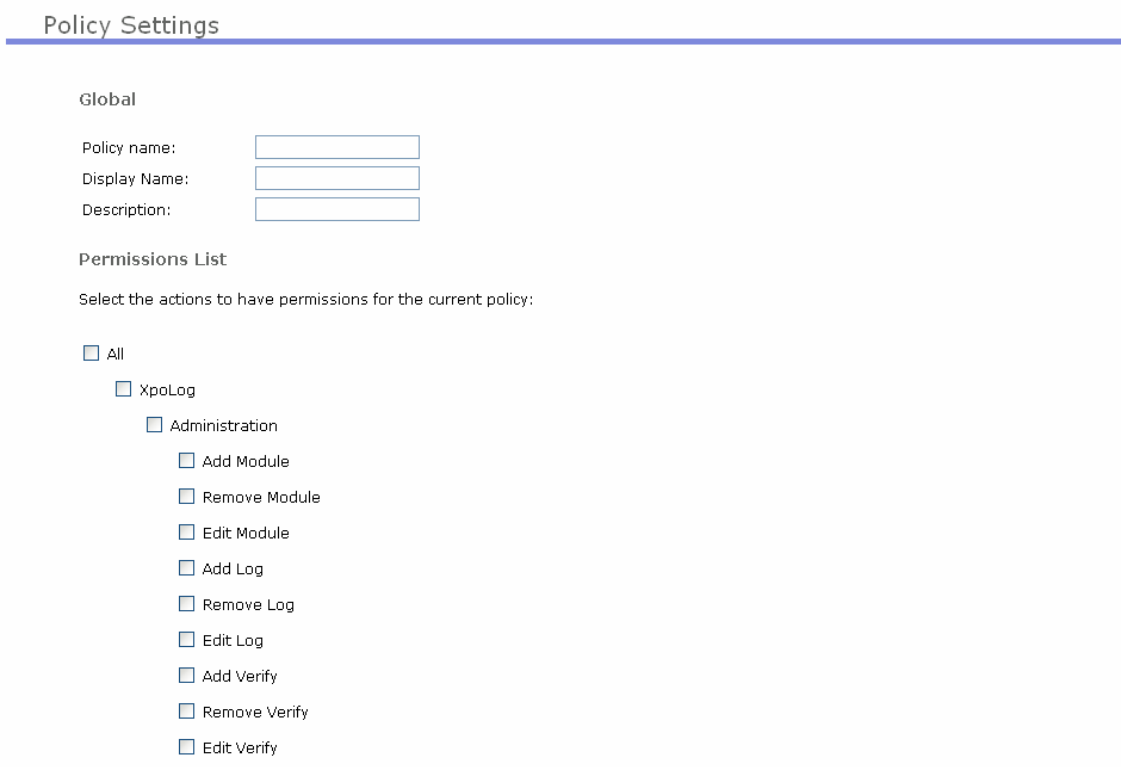
Policy Settings: specify the policy to be associated with the group. Select from using the policy of the groups to which the group is associated or select a specific policy.

Click the ‘Save’ link to save the new group definition.

Policies view



Click the ‘Add Policy’ link to create a new policy.



Specify the following details of the new policy:

Global

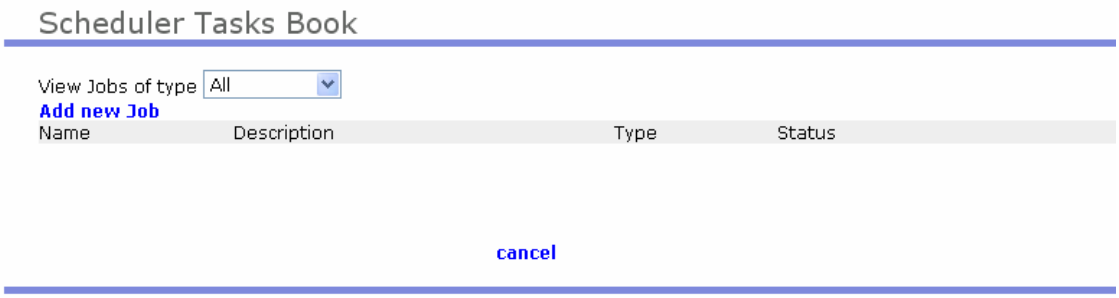
- **Policy name:** the name identifying the new policy.
- **Display Name:** the name that will be displayed across the system.
- **Description (optional):** the description of the new policy.

Permissions List: specify the permissions of the policy by choosing the components and allowed actions of each component. By leaving all check boxes unchecked a policy can define a view only permission for modules and logs and no permission for all other components in XpoLog.

Click the ‘Save’ link to save the new policy definition.

Automation Menu

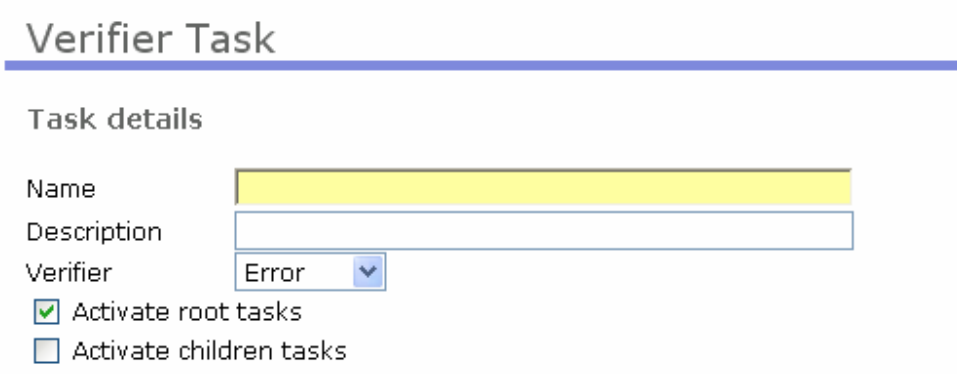
Scheduler



In order to add a new scheduled job click the 'Add new Job' link in the 'Scheduler Tasks Book' page. After clicking the link the following page will appear:

Define a new Verification Job

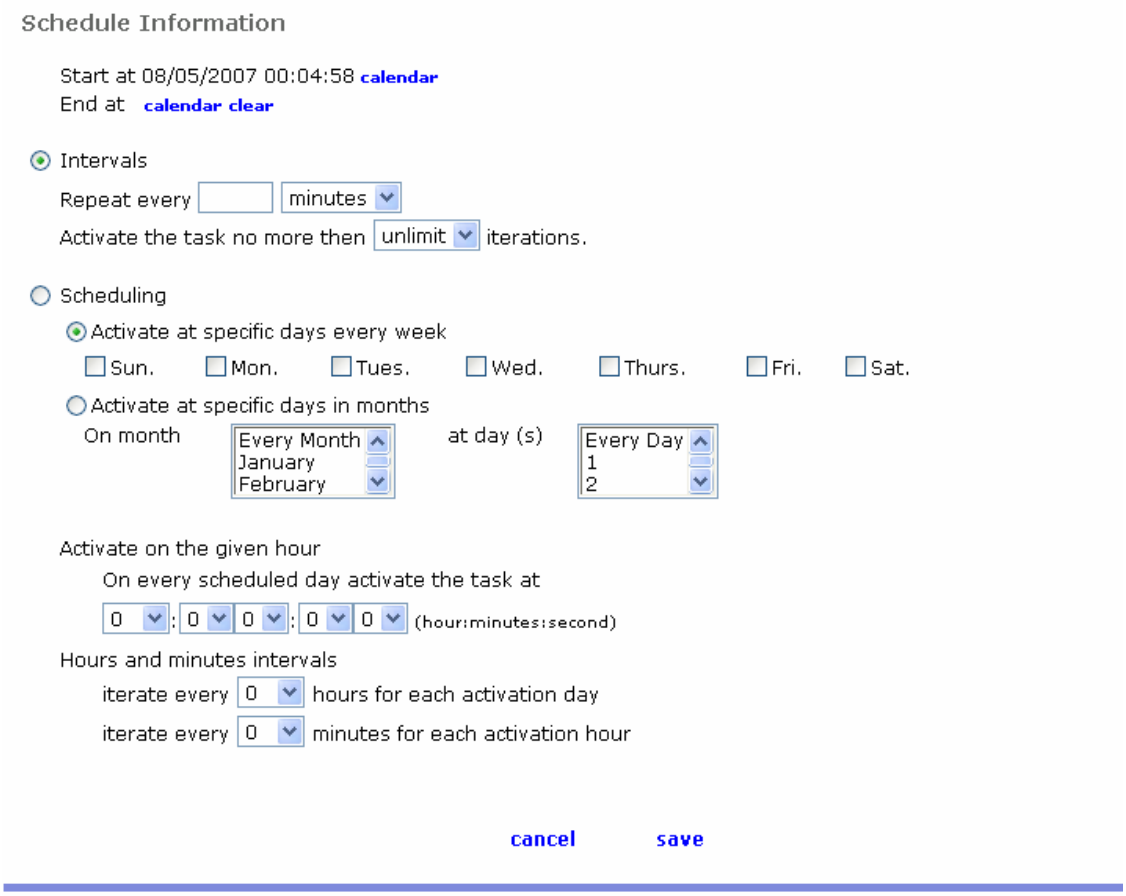
1. Click the 'Verification Job' link.
2. Task Details



- Enter the new scheduled task's name and description.
- Select the verifier to be activated by the scheduler from the 'Verifier' combo box.

- Check the 'Activate root tasks' check box to enable the events mechanism of the selected verifier.
- Check the 'Activate children tasks' check box if you want the tasks of the children verifiers (in cases of multi verifiers which are based on other verifiers) to be executed as well.

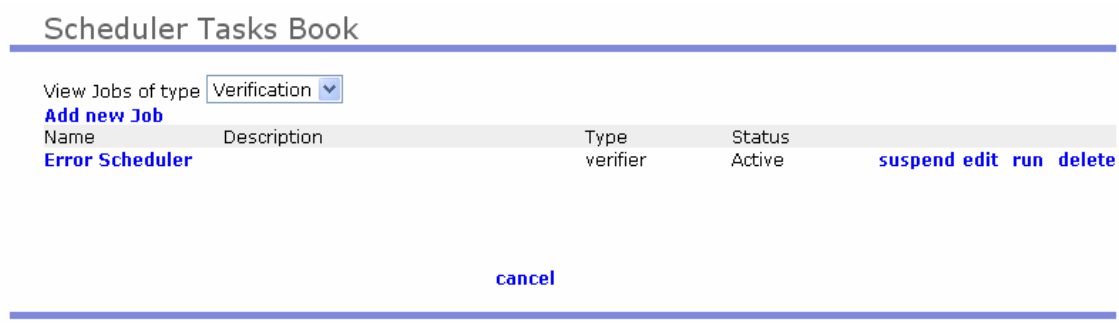
3. Schedule Information



- Click on the ‘calendar’ link of the ‘Start’ definition to specify future scheduling.
- Click on the ‘calendar’ link of the ‘End’ definition to specify the end time or leave blank for unlimited executions.
- Specify the scheduling information in one of two ways:
  - **Intervals**: execute the job at specific time intervals. Enter the number of hours, minutes or seconds that determine the interval and select whether the operation should be run only a number of times or should be unlimited.

- **Scheduling**: select either the days of the weeks in which the execution should take place, or specify the days of the month and the desired months in which you want your job to run.
  After defining the days at which your job should be executed define the time of desired executions. You can enter either a specific time (in the 'Activate on the given hour' section) or define hours interval and minutes interval (in the Hours and minutes intervals' section), so that on the selected days the operation will be executed in the given hours intervals and within each hour in the given minutes interval. For example, selecting in the scheduling section 'Every month' and 'Every day' and then defining to iterate every three hours and within each hour every 20 minutes will cause the job to be executed every at 00:20, 00:40, 01:00, 03:00, 03:20 and so on.

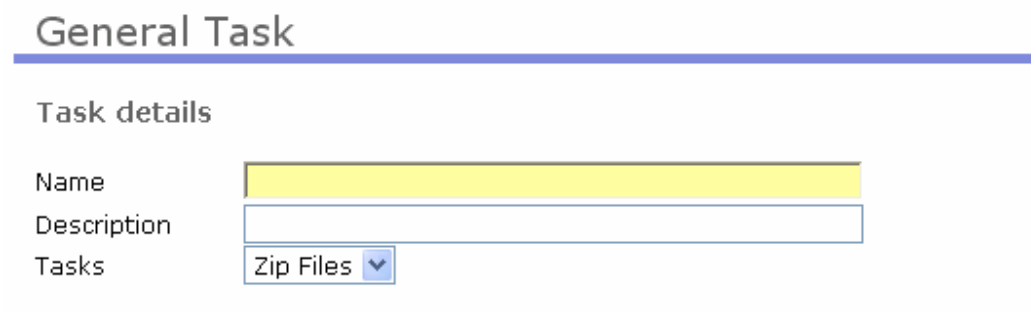
4. Click the ‘save’ link.



After saving, the scheduled verification job it is automatically active and will be executed according to the specified schedule.
Click the ‘suspend’ link to cancel future executions. Click the ‘activate’ link to reschedule future executions.
Click the ‘run’ link to force a single execution of the scheduled job.

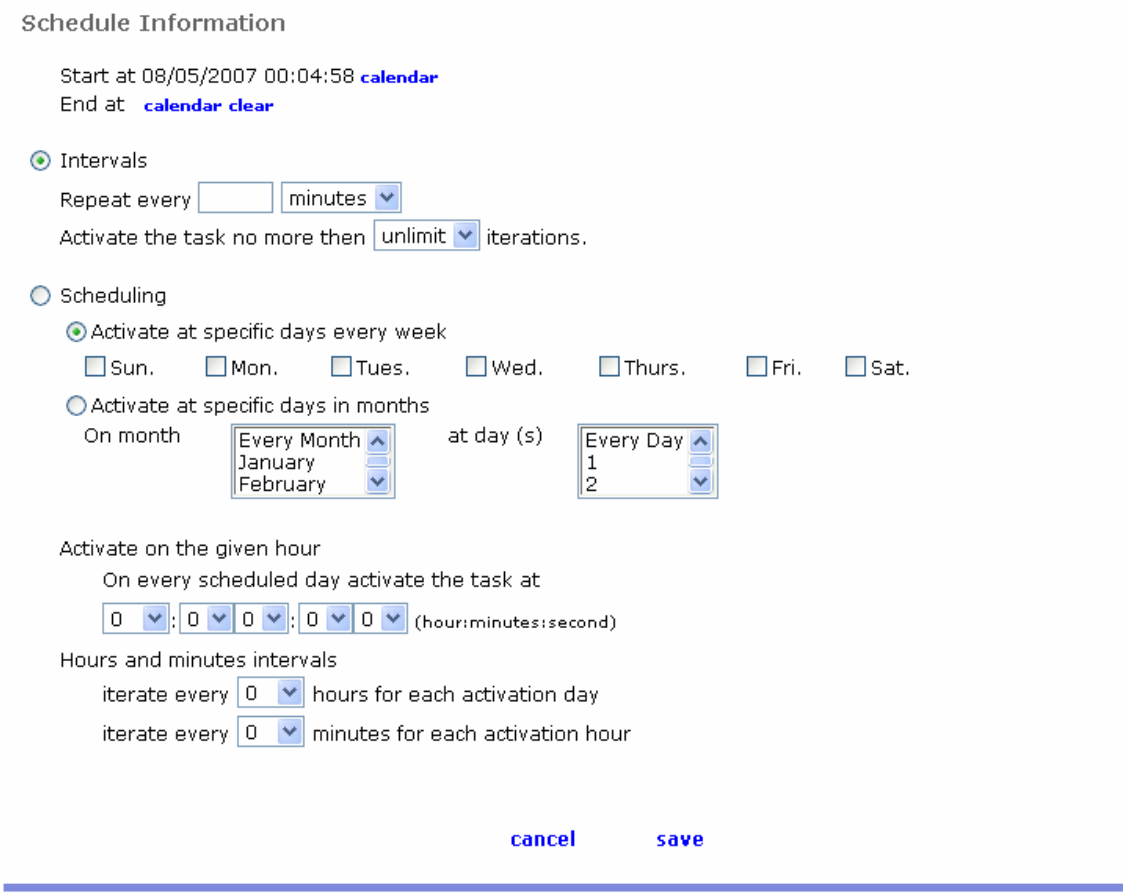
Define a new Operation Job

1. Click the ‘Operation Job’ link.
2. Task Details



   - Enter the new scheduled task’s name and description.
   - Select the task to be activated by the scheduler from the ‘Tasks’ combo box.

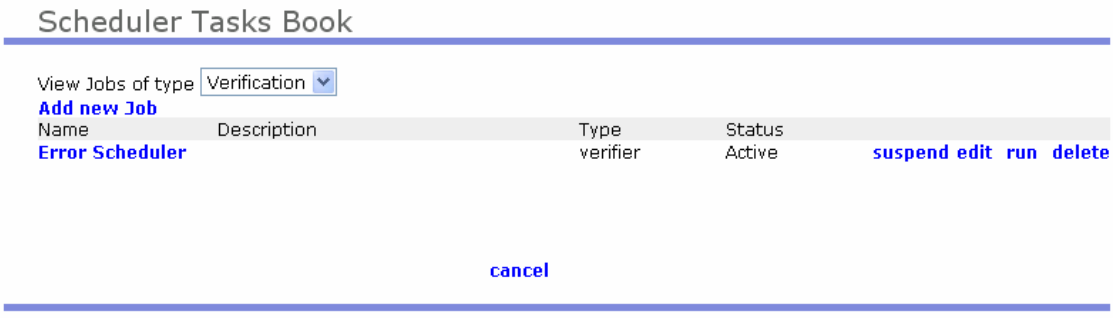
3. Schedule Information



   - Click on the ‘calendar’ link of the ‘Start’ definition to specify future scheduling.

- Click on the ‘calendar’ link of the ‘End’ definition to specify the end time or leave blank for unlimited executions.
- Specify the scheduling information in one of two ways:
  - **Intervals**: execute the job at specific time intervals. Enter the number of hours, minutes or seconds that determine the interval and select whether the operation should be run only a number of times or should be unlimited.
  - **Scheduling**: select either the days of the weeks in which the execution should take place, or specify the days of the month and the desired months in which you want your job to run.
    After defining the days at which your job should be executed define the time of desired executions. You can enter either a specific time (in the 'Activate on the given hour' section) or define hours interval and minutes interval (in the Hours and minutes intervals' section), so that on the selected days the operation will be executed in the given hours intervals and within each hour in the given minutes interval. For example, selecting in the scheduling section 'Every month' and 'Every day' and then defining to iterate every three hours and within each hour every 20 minutes will cause the job to be executed every at 00:20, 00:40, 01:00, 03:00, 03:20 and so on.

4. Click the ‘save’ link.

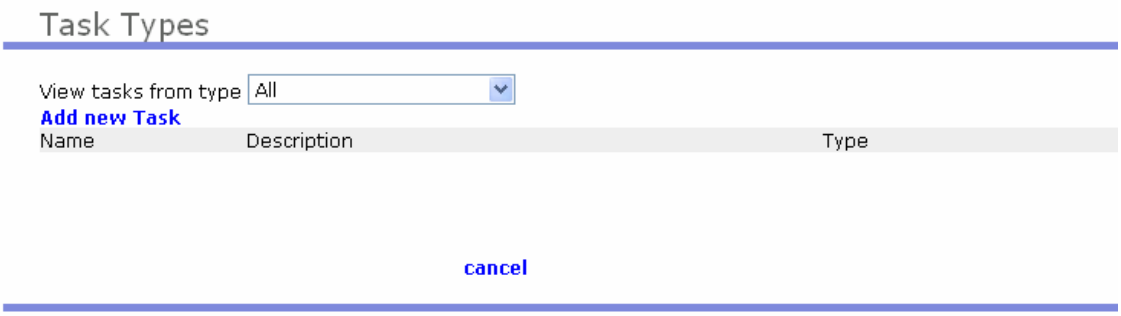


After saving, the scheduled operation job it is automatically active and will be executed according to the specified schedule.

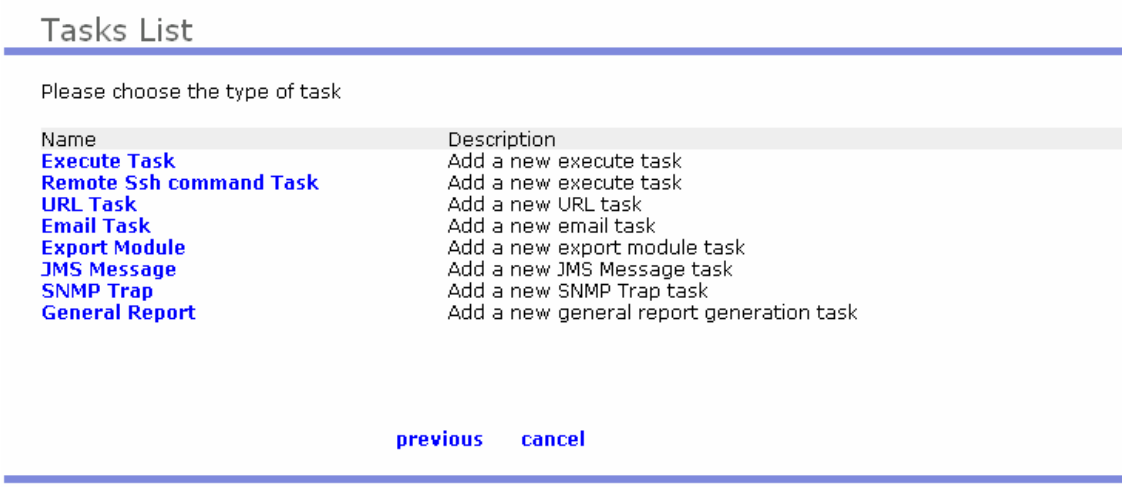
Click the ‘suspend’ link to cancel future executions. Click the ‘activate’ link to reschedule future executions.

Click the ‘run’ link to force a single execution of the scheduled job.

Tasks



In order to add a new task definition, click the ‘Add new Task’ link.



<u>Adding a new Execute Task</u>

1. Click the ‘Execute Task’ link from the ‘Tasks List’ page.

2. Specify the following configuration details:
   - **Name:** the name of the new task.
   - **Description (optional):** the description of the new task.

- **Program/Script path:** the name of the program/script to be executed by the task.
- **Arguments (optional):** the arguments needed for the program/script to run, separated by spaces.
- **Environment variables (optional):** the environment variables needed for the program/script to run.
- **Working directory (optional):** the directory from which the program/script should be run.
- **Output target file (optional):** the path to the file to which output of the program/script execution will be written.
- **Add optional params:** check to include the date, account name, host name and username in the output file.

3. Click the 'save' link to save the new task definition.

Adding a new Remote Ssh command Task

1. Click the 'Remote Ssh command Task' link from the 'Tasks List' page.

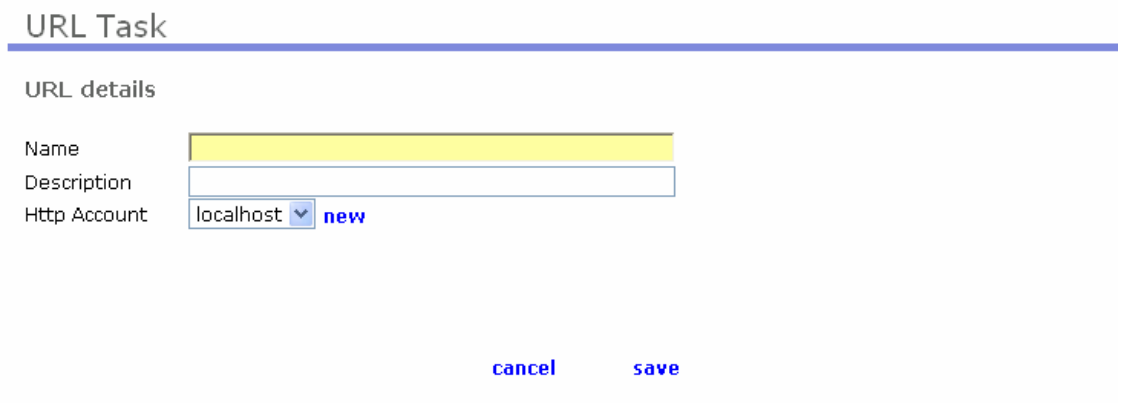
2. Specify the following configuration details:
   - **Name:** the name of the new task.
   - **Description (optional):** the description of the new task.
   - **Ssh account:** the account of the host on which the program/script will be executed.
   - **Program/Script path:** the name of the program/script to be executed by the task.
   - **Arguments (optional):** the arguments needed for the program/script to run, separated by spaces.

- **Environment variables (optional):** the environment variables needed for the program/script to run.
- **Output target file (optional):** the path to the file to which output of the program/script execution will be written.
- **Add optional params:** check to include the date, account name, host name and username in the output file.

3. Click the ‘save’ link to save the new task definition.

Adding a new URL Task

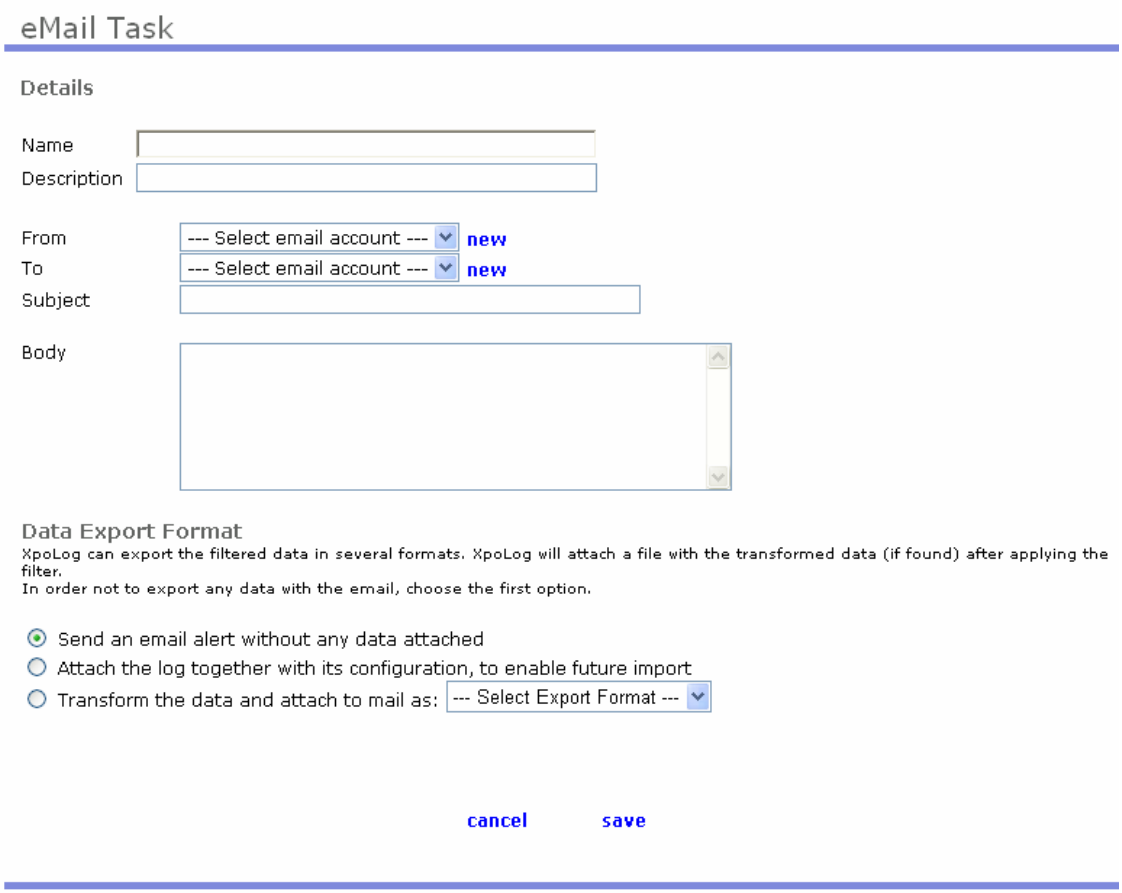
1. Click the ‘URL Task’ link from the ‘Tasks List’ page.



2. Specify the following configuration details:
   - **Name:** the name of the new task.
   - **Description (optional):** the description of the new task.
   - **Http account:** the account on which the program/script will be executed.
3. Click the ‘save’ link to save the new task definition.

Adding a new Email Task

1. Click the ‘Email Task’ link from the ‘Tasks List’ page.



2. Specify the following configuration details:
   - **Name:** the name of the new task.
   - **Description (optional):** the description of the new task.
   - **From:** the account from which the email will be sent.
   - **To:** the account to which the email will be sent.
   - **Subject:** the subject of the email.
   - **Body (optional):** the body of the email.
   - **Data Export Format:** select the format of the email attachment:
     - No attachment.
     - Attach log data and configuration.
     - Attach log data in specific format (XML, CSV or TAB Delimited).
3. Click the ‘save’ link to save the new task definition.

Adding a new Export Module Task

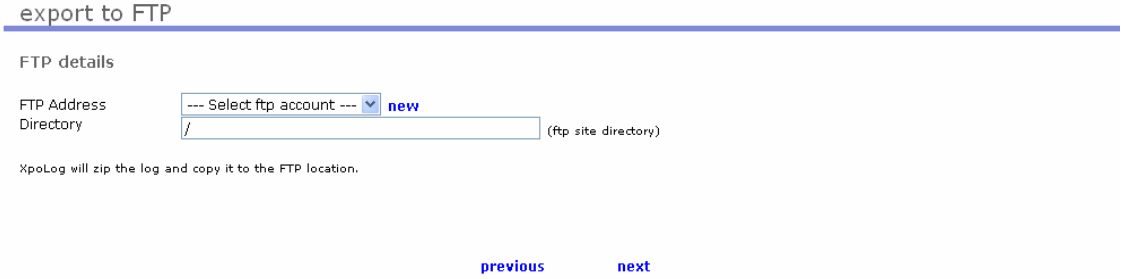
1. Click the ‘Export Module’ link from the ‘Tasks List’ page.

2. Select modules and logs to be exported by the task.
3. Click the ‘next’ link.
4. Select the exporting media.

- **Zip and send by email**

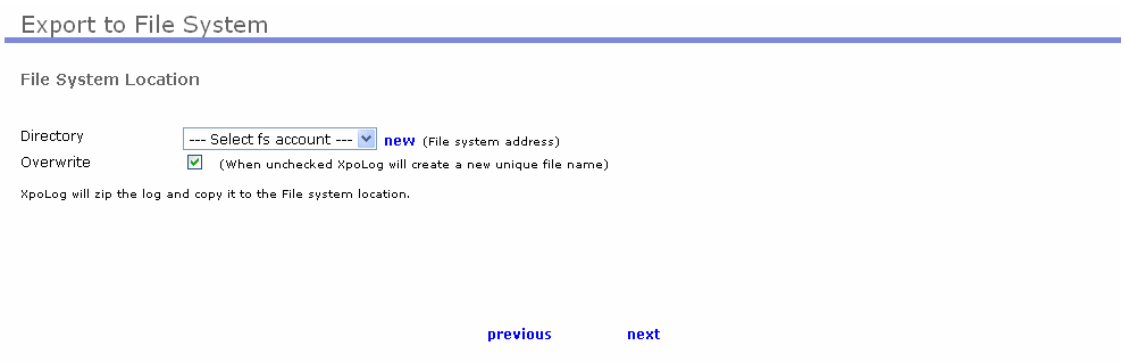
  - Specify the following configuration details:
    - **From:** the account from which the email will be sent.
    - **To:** the account to which the email will be sent.
    - **Subject:** the subject of the email.
    - **Text (optional):** the body of the email.
  - Click ‘next’.
  - Specify the new task’s name and description.
  - Click ‘save’ to save the new task.

- **Zip and send by ftp site**



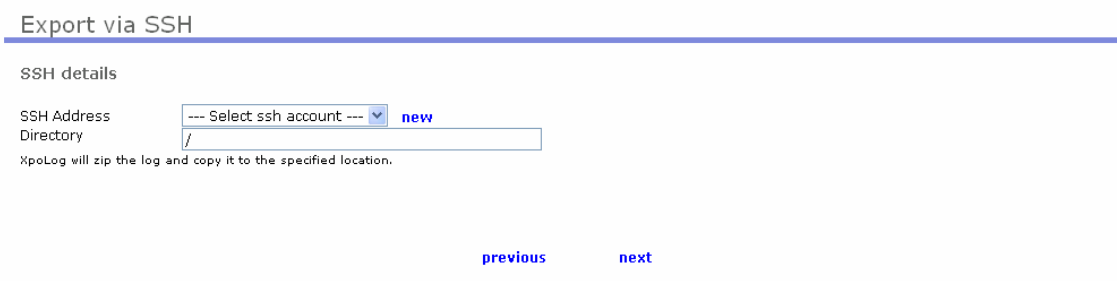
  - Specify the following configuration details:
    - **FTP Address:** the account of the ftp site.
    - **Directory:** the directory the exported modules and logs will be uploaded to.
  - Click ‘next’.
  - Specify the new task’s name and description.
  - Click ‘save’ to save the new task.

- **Zip and copy to a local file system address**



  - Specify the following configuration details:
    - **Directory:** the account pointing to the file system location to which the exported modules and logs will be saved.
    - **Overwrite:** indicates whether the zip file should overwrite a duplicate file or create a new file with unique name.
  - Click 'next'.
  - Specify the new task's name and description.
  - Click 'save' to save the new task.

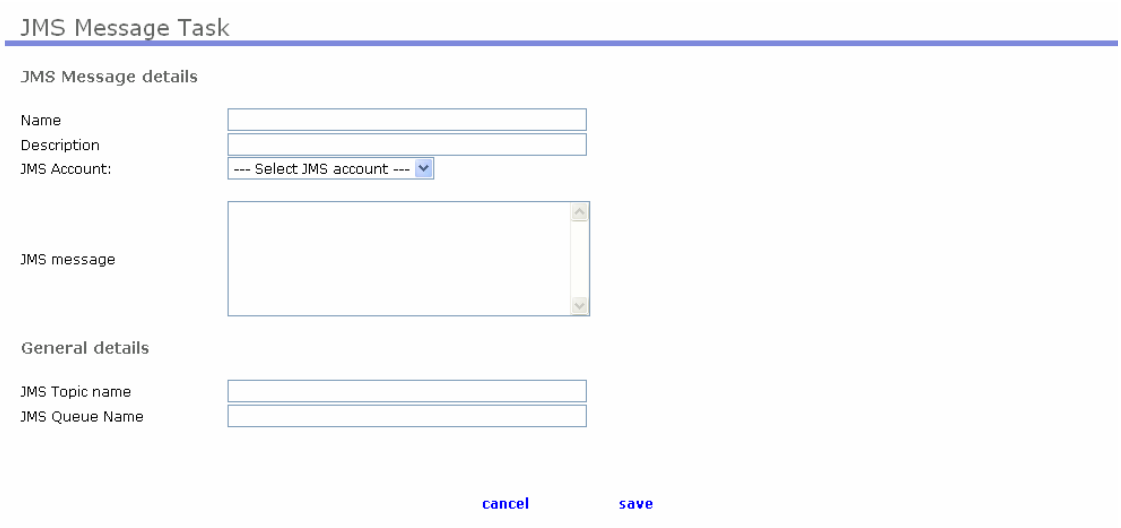
- **Zip and copy to remote machine via SSH**



  - Specify the following configuration details:
    - **SSH Address:** the SSH account of the remote host.
    - **Directory:** the directory the exported modules and logs will be uploaded to.
  - Click 'next'.
  - Specify the new task's name and description.
  - Click 'save' to save the new task.

Adding a new JMS Message Task

1. Click the 'JMS Message' link from the 'Tasks List' page.

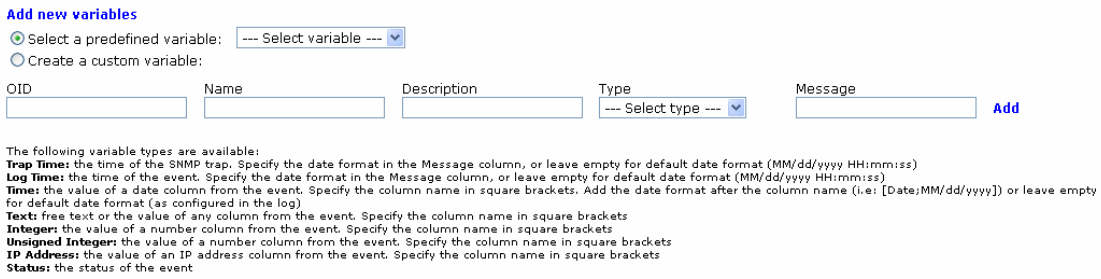


2. Specify the following configuration details:
   - **Name:** the name of the new task.
   - **Description (optional):** the description of the new task.
   - **JMS Account:** the JMS account to be used.
   - **JMS message:** the JMS message to be written.
   - **JMS Topic name (optional if JMS Queue name was specified):** the name of the JMS topic the message should be written to.
   - **JMS Queue name (optional if JMS Topic name was specified):** the name of the JMS queue the message should be written to.
3. Click the 'save' link to save the new task definition.

Adding a new SNMP Trap Task

1. Click the ‘SNMP Trap’ link from the ‘Tasks List’ page.

2. Specify the following configuration details:
   - **Name:** the name of the new task.
   - **Description (optional):** the description of the new task.
   - **SNMP Account:** the account to be used.
   - **SNMP Trap OID (optional for account of version 1):** the OID of the SNMP trap.
   - **SNMP Community (optional):** the target community.
3. Specify the SNMP trap variables:
   - Click the ‘Add new variables’ link.



   - Add new variables, either by selecting from the predefined variables’ list or by specifying the custom details of the variable:
     - **OID**: the OID of the variable.
     - **Name**: the name of the variable.
     - **Description (optional)**: the description of the variable.
     - **Type**: the type of the variable.

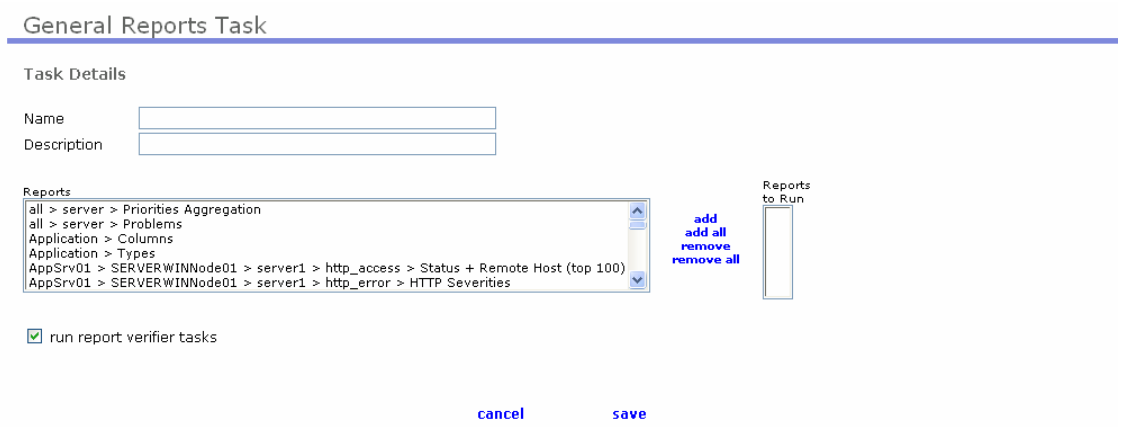
- **Message:** the message to be sent in the trap. This field is a dynamic field, which can contain placeholders which can be replaced with data from the log. The available placeholders are determined by the type of the variable in the following manner:
    - **Trap Time:** the time of the SNMP trap. Specify the date format in the Message column, or leave empty for default date format (MM/dd/yyyy HH:mm:ss).
    - **Log Time:** the time of the event. Specify the date format in the Message column, or leave empty for default date format (MM/dd/yyyy HH:mm:ss).
    - **Time:** the value of a date column from the event. Specify the column name in square brackets. Add the date format after the column name (i.e: [Date;MM/dd/yyyy]) or leave empty for default date format (as configured in the log).
    - **Text:** free text or the value of any column from the event. Specify the column name in square brackets.
    - **Integer:** the value of a number column from the event. Specify the column name in square brackets.
    - **Unsigned Integer:** the value of a number column from the event. Specify the column name in square brackets.
    - **IP Address:** the value of an IP address column from the event. Specify the column name in square brackets.
    - **Status:** the status of the event.

o Click the 'Add' link to add the new variable to the existing variables' list.

4. Click the 'save' link to save the new task definition.

<u>Adding a new General Report Task</u>

1. Click the 'General Report' link from the 'Tasks List' page.



2. Specify the following configuration details:
   - **Name:** the name of the new task.
   - **Description (optional):** the description of the new task.
   - **Reports:** select the report to be executed by the task.
   - **run report verifier tasks:** check to indicate that report verifiers should be executed as well.
3. Click the ‘save’ link to save the new task definition.

XpoSearch

Search Engine

Starting with version 2.7, XpoLog comes with a search engine that supports rapid textual search in logs. This enhanced search capability is integrated both in the log viewer (utilized by the filters and the quick search) and in a search engine screen that enables to search for text within multiple logs. The search engine search capability is based on an indexing mechanism that can run both automatically and upon user request. Only indexed logs are used by the search engine.

Running a Search

Click the Search Engine component to enter the search portal.
You can perform both simple, straightforward searches and advanced searches. For a simple search, simply enter the search term in the 'Search for' text box and press enter or click the 'go' link. Writing down a single word or a list of words will cause XpoLog to search all logs in which at least one of the words appear (OR operation). You can also define a regular expression as a search term. Searching a regular expression allows you to use wildcards anywhere within the search term, but it might cause for longer search times - especially if the wildcards appear at the beginning of the search term.

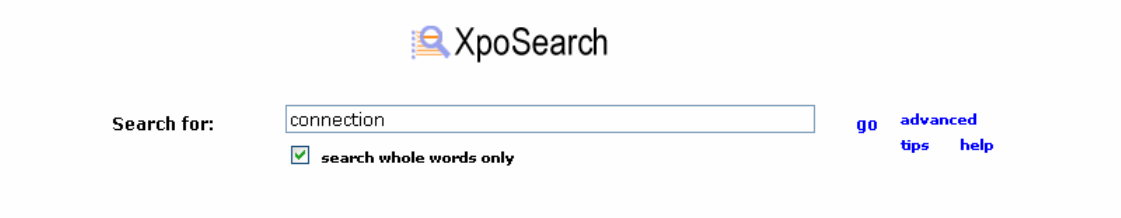


Figure … - XpoSearch search portal

The result of a search query is a list of logs with indexing information and log information displayed next to each log result. By clicking on a search log result you drill down to that log's log view, where only records containing the search term are displayed. To get a merged view of the result logs select the 'Merge results' link in the results status line. Select the logs you want to participate in the merged result. By clicking the 'view' link, XpoLog will create a temporary merge log based on the selected logs and will show

it in the log view. Clicking the 'save and view' link will create and save the merge log and will then open its log view.

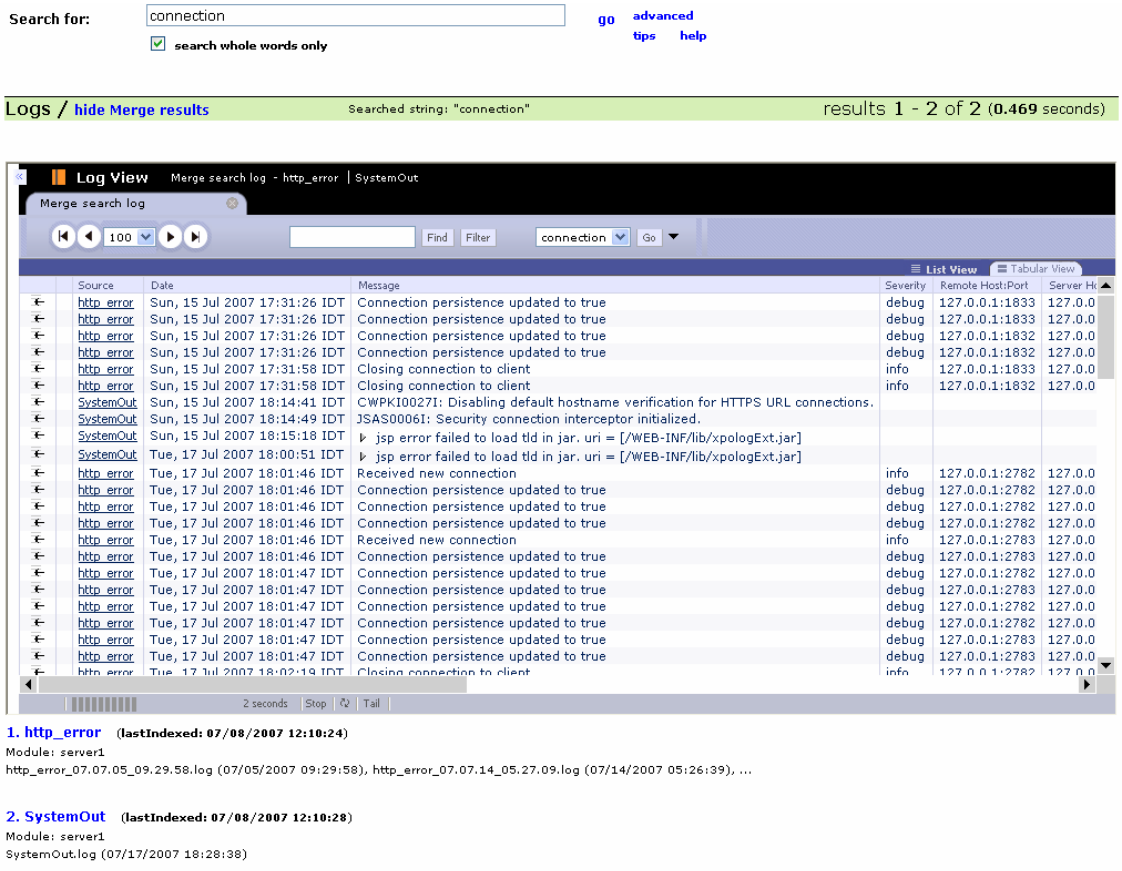


Figure … - Search result logs merged view

Clicking on the 'advanced' link will open the advanced search information section. If a different number results per page is desired, override the search engine default in the 'Results per page' entry.

If you want to search for logs where all the search terms appear, select in the 'Find Results' section the 'with all of the words' option. Otherwise use the 'with at least one of the words' option.

In the 'Search in' section, selecting 'only selected logs' will display the 'Select indexed logs' link that opens the logs tree. Only logs which use indexing and have been indexed will appear in that tree. Select the logs and modules to participate in the search. Click on the 'Hide selected logs' to hide the logs tree.

By default XpoLog searches the search term only within its own logs. To perform the

search also on logs residing in remote XpoLog nodes, select these nodes in the XpoLog nodes list in the 'Search on' section.

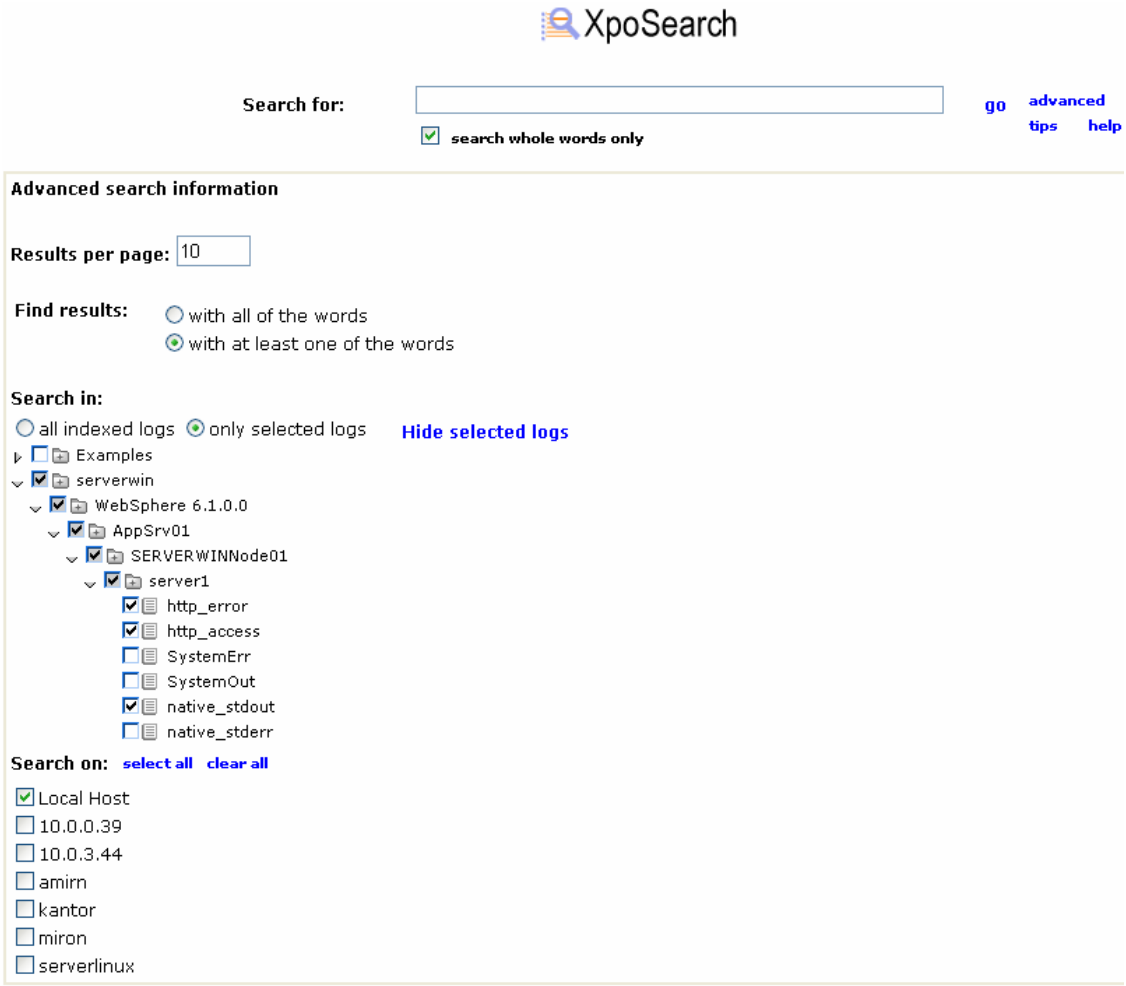


Figure … - Advanced search options

Running a search with a given search term will create a new 'user search result' entry that will be displayed in the 'Search Results' slide of the management pane on the left side of the screen. This way you can return to previously performed searches. Right click a search result and select 'Remove search' to remove it from the search results list, or click the small arrow in the 'Search Results' slide title and select 'Clear searches' to delete all pervious searches.

Administration

Click the 'XpoSearch' component to enter XpoLog's search engine. Select the 'Administration' menu to enter the 'Search Engine Management' screen. The search engine management information is organized in 4 tabs:

Log Selection

Select the logs you want to be indexed. Click 'save' to save your changes.

Global Scheduler

Set here the automatic execution of the global scheduler that will index logs for the first time. Select the 'Enable indexing scheduler' option to turn on the scheduler. See ‘schedule information’ for more information on how to set a scheduler. The default indexing scheduling definition is to run every night, at 1 AM.

Delta Scheduler

Set here the automatic execution of the delta scheduler that will update the index of already indexed logs. Select the 'Enable delta indexing’ option to turn on the scheduler. See ‘schedule information’ for more information on how to set a scheduler.

General -

- Number of results per page: enter here the number of log results to be displayed in each result page of a search.
- Minimal file change: the minimal size in bytes of the changed or added portion of a log in order for the log to be indexed during delta scheduler executions.
- Average CPU Limitation: the average CPU consumption for indexing. Setting any value other than 'Unlimited' will influence the indexing performance.
- Indexing directory: either the default indexing directory or a user defined directory. Changing this setting will move all indexes to the selected directory; if this setting is done while a log is being indexed, that index will be deleted.
- Index numbers: check this value to enable indexing of numerical values.

Special characters: enter a sequence of all the characters that should serve as token delimiters and not be indexed. Use this option if you don't want to index certain characters. Since the indexed tokens are smaller in case special characters are used, the resulting indexing is smaller and the overall performance of the search engine increases.

Indexing

Log indexing is the process of scanning a log and creating an index - the structure that holds the information needed to quickly search for a text. In order to index a log, you need to turn on its 'use indexing' option. By default, all newly created logs have this option set. Most logs created by wizards also have this option set. Setting the 'use indexing' option can be done from 3 separate locations: from the log administration, the log customization and the search engine administration. Certain log types, such as remote logs, do not support indexing (remote logs could then be indexed on the XpoLog node on which they are defined).

Manual Indexing

On top of running log indexing using the scheduler as defined in the search engine administration you can also run logs indexing manually. To run manual indexing, do the following:

1. Click the 'XpoSearch' component and select the 'Indexing' menu to enter the 'Search Engine Indexing' screen.
2. Select from the logs tree the logs you want to index and click the 'run' link.
3. An 'indexing started running' message will be displayed. Press 'ok' to return to the indexing page. The status of the current log being indexed is displayed in the upper part of the view and in the log tree.

In the log view, if a filter was activated or a search term was entered and the log is set for indexing, a message prompting the user to run an index update will pop up in case the index is not up-to-date.

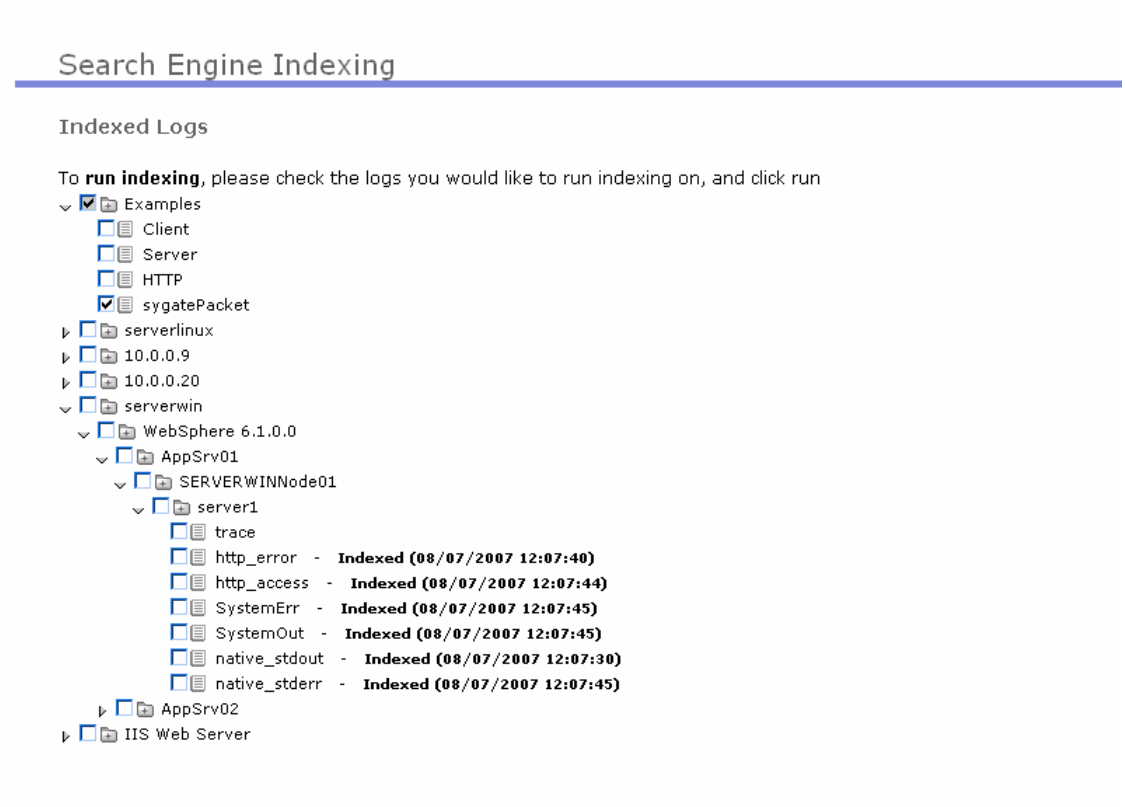


Figure … - Search engine indexing

Dashboard

Health view

XpoLog Dashboard is a component which allows you to get a high level picture of your entire system by displaying an overview of the health state of the different components in your system. Health is measured both in the occurrence of log events correlating to certain problems in your system ('risk') and in anomalies in log files - such as in the case where many events are suddenly written to a log file, something that may denote a problem in that log file's application. The dashboard's user interface enables the user to drill down both in the components resolutions (traversing an application by its modules tree, finally getting to the applications logs and their filters) and the time frame displayed (drill down from a time frame of one month to a day and then to an hour). From the component's lowest level (a log, a log's filter or a log's column) you can drill down directly to the log view of that log and continue your analysis there.

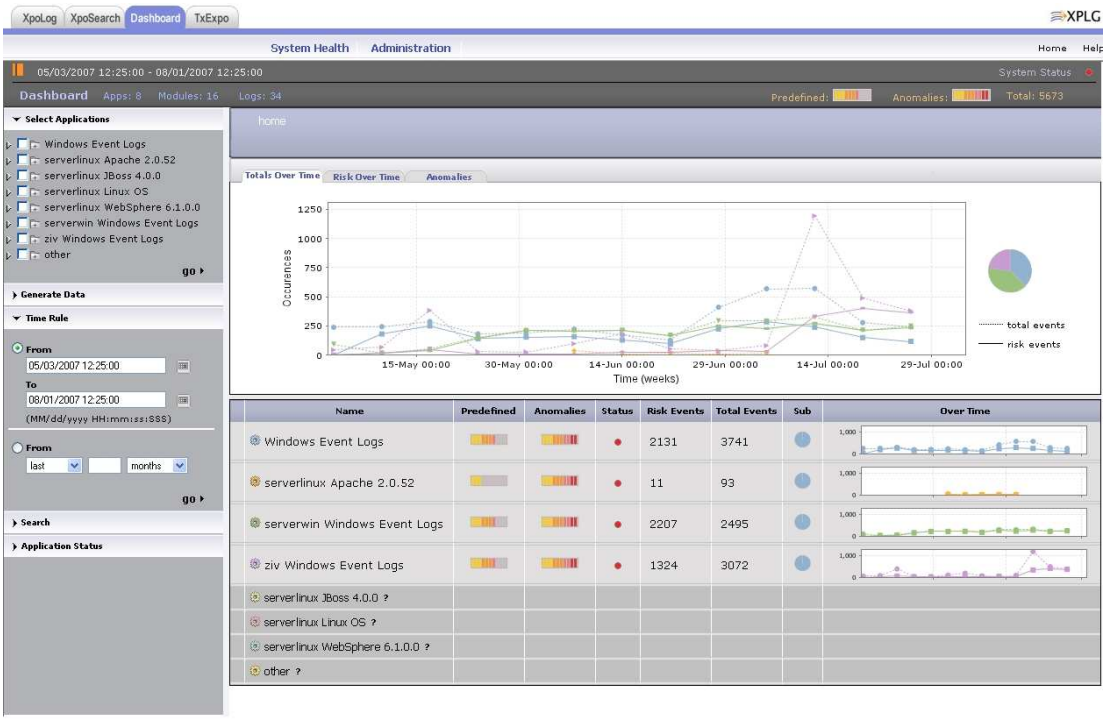


Figure … - System Health Screen

The first time you enter the health view screen (by selecting ‘Dashboard’ from the portal or by clicking the ‘Dashboard’ tab) XpoLog collects the dashboard data based on the time frame defined in the dashboard administration; collecting the health view data might take

a couple of minutes, based on the amount of data. If you leave the health view screen the current display setup is saved, so next time you enter it you get the same view.
The health view screen is divided into three panes:

- The upper pane displays general information about your system, such as the number of applications, modules and logs defined, a general status indication, indications for the level of risk and anomalies, and the time frame of the viewed dashboard.
- The left pane is a control pane that comprises of five slides – for selecting the viewed applications, for setting the time rules for displayed and generated data, for entering a search query and for displaying the top level (application level) health state of your system. Use this control pane to navigate both in time and both between applications.

Select Applications

This slide displays the application tree of your system: applications, modules, and logs in a hierarchical view.

- Selecting a root for the displayed data: simply click on any component in the tree. The view in the main pane will be refreshed accordingly.
- Correlating the health state between different components: select the desired components from the tree and click ‘go’. The view in the main page will refresh showing only the selected components, as the figure below illustrates:

Figure … - Correlated System Health View of Windows Event Logs

Generate Data

Use this slide to define the time frame to generate new data for. Enter either ‘from/to’ values or enter ‘last/previous’ data to define the time frame. If you want to generate data on selected components only, select them in the tree above and check the ‘only selected apps’ option; otherwise leave this option unselected. To start generating data, click the ‘go’ link.

Generating data might take a while, depending on the amount of data in your logs, the time frame set and the components selected.

The figure bellows demonstrated the settings for generating data for the last 3 months for the applications ‘serverlinux Apache 2.0.52’, ‘serverlinux JBoss 4.0.0’ and ‘serverlinux Linux OS’:

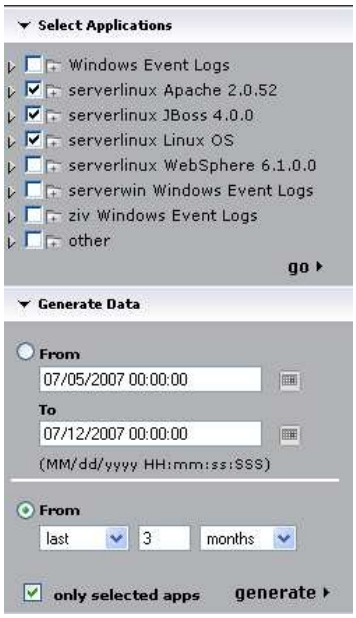


Figure … - Generate Data

Time Rule

The ‘Time Rule’ slide is used to define a new time frame for the viewed data. Set the time frame exactly as you set the time frame for data generation and click ‘go’ to refresh the view. Notice that missing data will not be generated – only already available data for the specified time frame will be processed and displayed.

Search

Enter here a search phrase and click ‘go’ to get the search results in a new XpoLog page.

Application Status

This slide displays a summary of the system health of the upper most level the components tree – the applications. Clicking an application has the same affect as clicking an application in the application tree – setting the application to be the root of the system health display in the main pane.

Main Page

The main pane consists of two parts: the upper one shows an over (main) time graph of the selected mode (totals over time, risk over time and anomalies), and the lower part contains a table with information and graphs of the children of the selected component. If you click on a node in the main graph you will drill down to the time frame displayed in that node’s tool tip as show below:

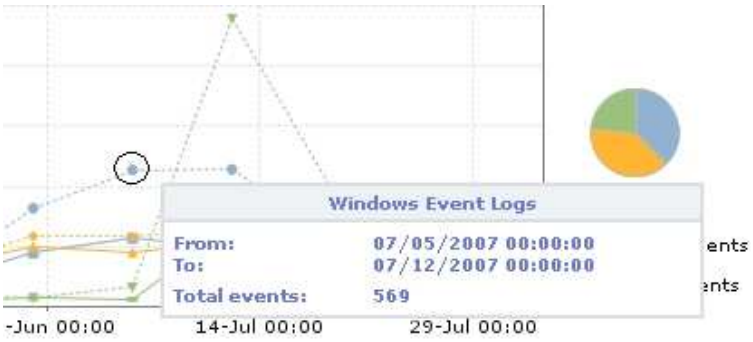


Figure … - Graph Node Tool Tip Data

Clicking on the marked node will result in the following view:

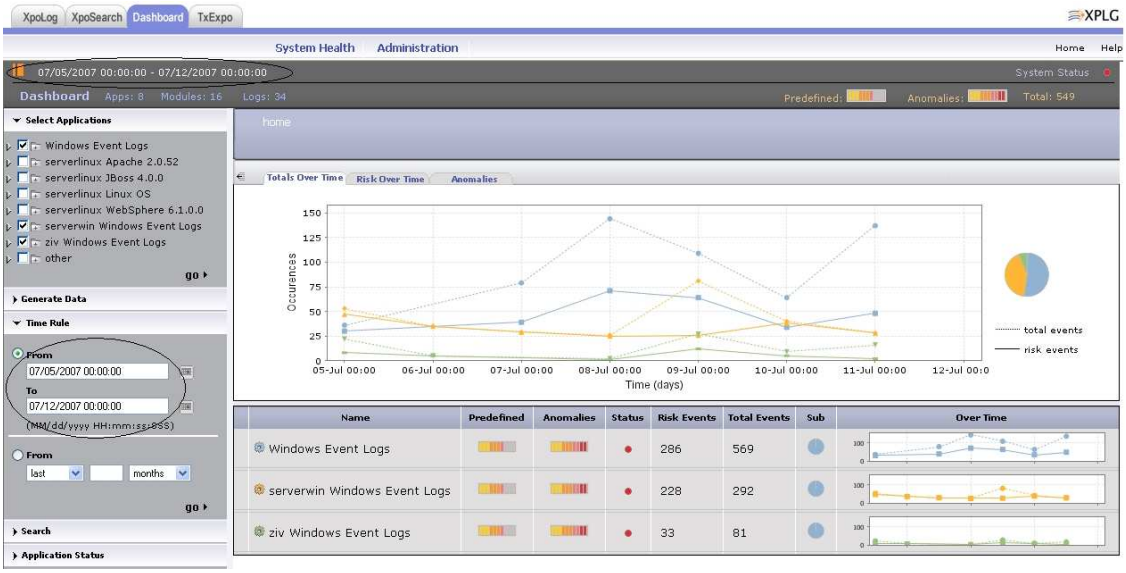


Figure … - Time Frame Zoom In

Do return to the pervious time frame, simple click on the arrow next the ‘Totals Over Time’ tab.

The entries in the table below the graph are divided into two groups: the components with a light grey background are those with data (although the might have no risk or anomalies). The components with a dark grey background are those for which no system health data is available. To generate data for these components, select them in the components tree in the control pane on the left, enter the time frame desired in the ‘Generate Data’ slide (**not** the ‘Time Rule’ slide) and press ‘go’. When hovering with the mouse of the question mark next to a component for which no data is available, an appropriate message is displayed as shown in the picture below:

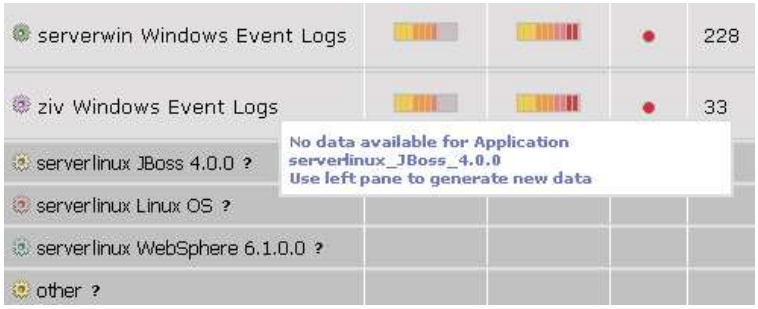


Figure … - No Data Message

Administration

As described earlier, the system health is measured both in terms of risk and in terms of anomalies. Both risk and anomaly definitions can be set for each and every log in your system.

Defining log risks

Risks for a log are defined as the occurrence of certain events in that log. For instance, the occurrence of an access log event with a 404 status may denote that an illegal request has been submitted. Or an event of an error log with a priority "FATAL" means something pretty bad happened in your application.

To isolate these events, XpoLog uses a set of filters, each corresponding to an event or a multitude of events. From the log view select from the log navigation bar the filter's menu by pressing the small arrow next to the filter's "go" link. Select "edit" to edit an already defined filter or "new" to create a new one. For more information on defining filters, see **Filter Definition**. In the filter definition page, the last section is called "System Health". This is where you set the risk level that corresponds to the occurrence of (one or more) events defined by that filter. The lowest risk is 1 and the highest is 10. If the event denoted by that filter does not mean any risk to your system, leave the risk weight at "None". For instance, in an error log containing priorities, you might set a filter called "FATAL" by selecting the "FATAL" entry of the "Priorities" section in the filter definition page, and set the risk weight to be 10.

To complete the System Health definition enter the condition for the given risk weight by selecting the number of events and the operation (more then, less then, equals and not equals). The condition defines the number of occurrences of that log within the minimal time frame of **5 minutes**. For instance if the occurrence of at least 5 error events in an error log in a time frame of five minutes means a risk weight of 8, select 8 at the risk weight, "More Then" in the next combo box and enter "4" in the text box to complete your definition.

Log's configurations in XpoLog generated either by the detection wizard or by running an application wizard have already their risk levels set for their predefined filters. You can always edit these filters to change their risk level or enter new filters with new risk

levels that correspond to events you consider risky.

The picture below displays an example of setting such a filter:

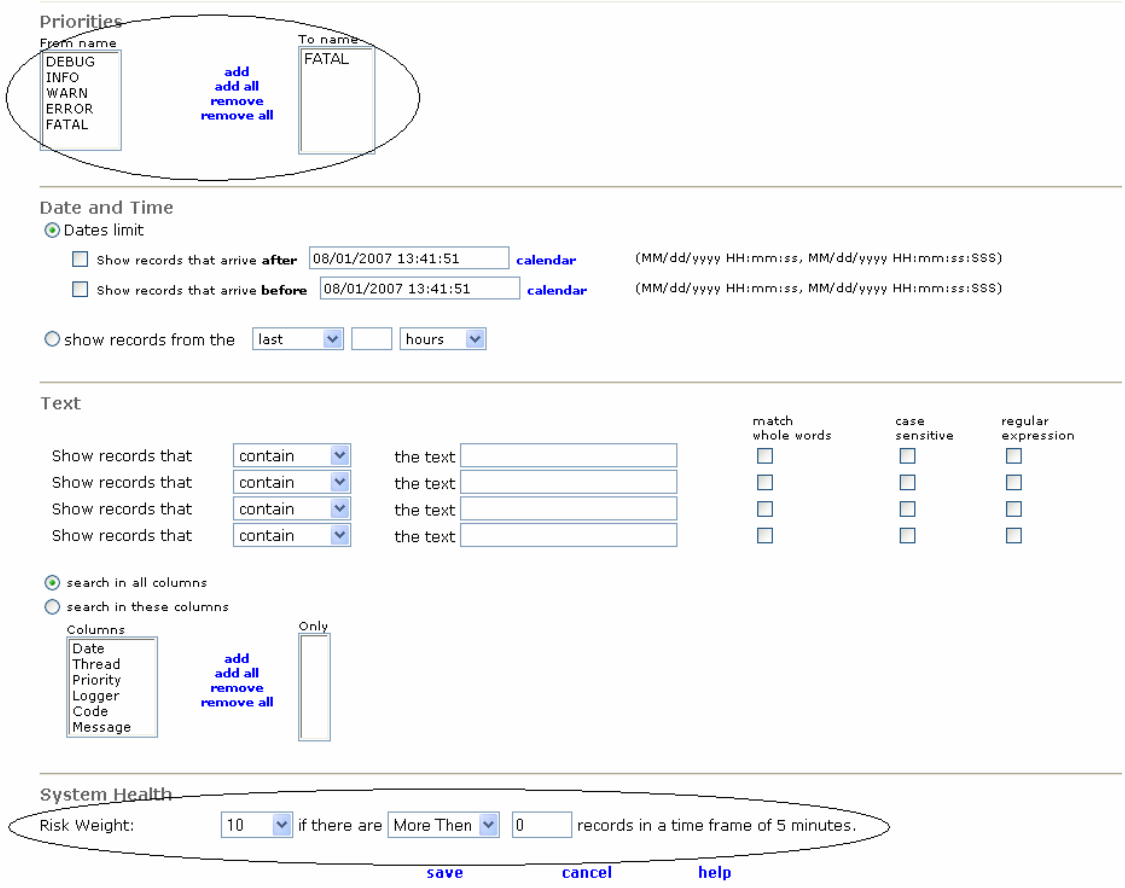


Figure … - Defining Log Risks

In the dashboard administration screen you can set the risk weights of multiple filters together. To set risk levels for multiple filters, do the following:

1. Select the ‘Dashboard’ component and then ‘Administration’ from the top menu to enter the dashboard’s administration page.
2. In the ‘System Filter Rules’ set the system health as described above, select from the logs' tree the filters you want this health setting to apply to and click ‘save’. If you want to set further risk setting for other filters, just repeat these steps and click ‘save’ again.

3.

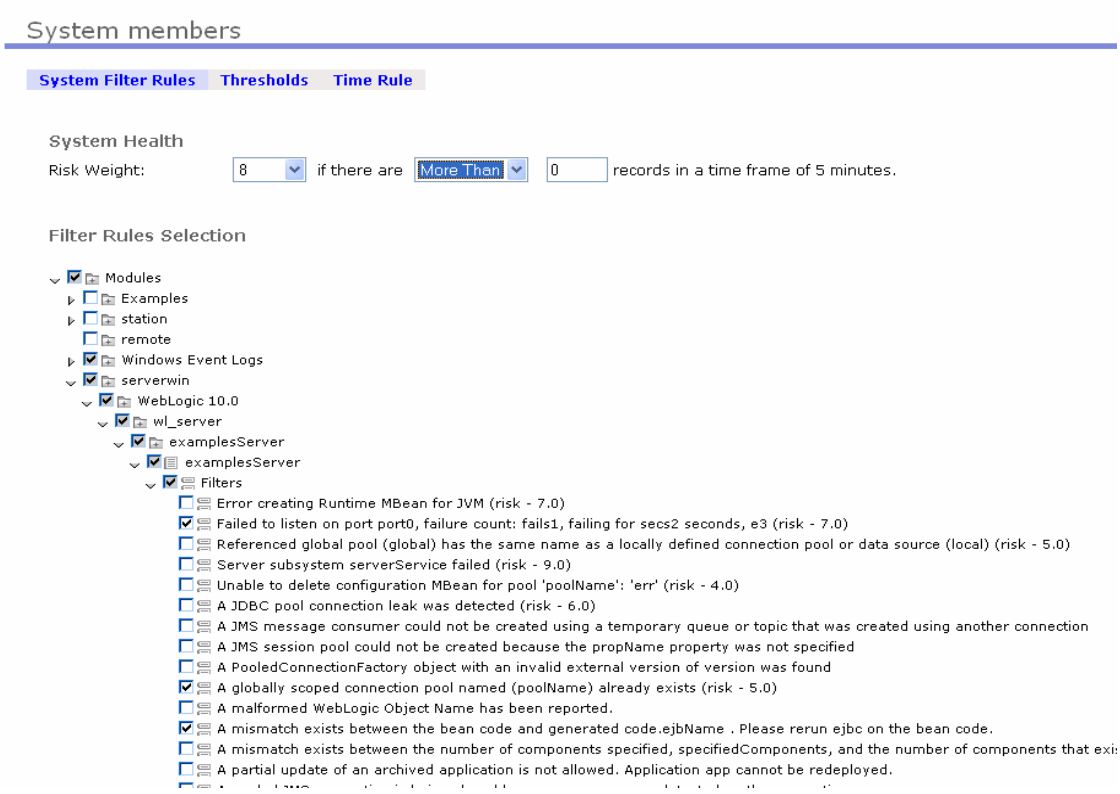


Figure … - Setting risk weight for multiple logs

Defining log statistics

Anomalies are defined as deviations in terms of the number of occurrences with relation to previously computed averages. Statistics for logs is computed for every hour of the week and takes into account both the number of total events of the log and the number of unique occurrences of values for selected log columns ("Column statistics"). For more information on statistics and anomalies, see the 'Defining log statistics' section of the help.

In order to set the statistics parameters of a certain log, do the following:

1. Go to the log's edit wizard. See 'Log Configuration' for more details on how to define logs. Click 'next' in the Log's general definition's page to get to the 'Log pattern administration' page and click 'next' again here to get to the 'Log field admin' page.
2. In the 'statistics settings' section, select the 'Compute statistics' option to enable statistical evaluation of the log. When this option is selected, the 'Compute statistics' combo box is displayed next to each of the log's fields (columns). For

each column you want statistics (and anomalies) to be computed for select one of the following options:

a. ‘Do not compute’ – no statistics (and no anomaly) will be computed for this column.
b. ‘Compute unique values’ – statistics will be computed for each of this column's values.
c. ‘Compute average’ – only the average of the occurrences of unique values will be computed. Anomaly for each unique value is then computed based on this average statistics.

Selecting ‘compute unique values’ for a column where many unique values are expected will result in large statistics data and less accurate anomalies, so always consider in these cases using ‘compute average’. In the image below statistical evaluation for the log was turned on, average statistics computation was defined for the ‘Source IP’ column and unique values statistics computation was defined for the ‘Status’ column

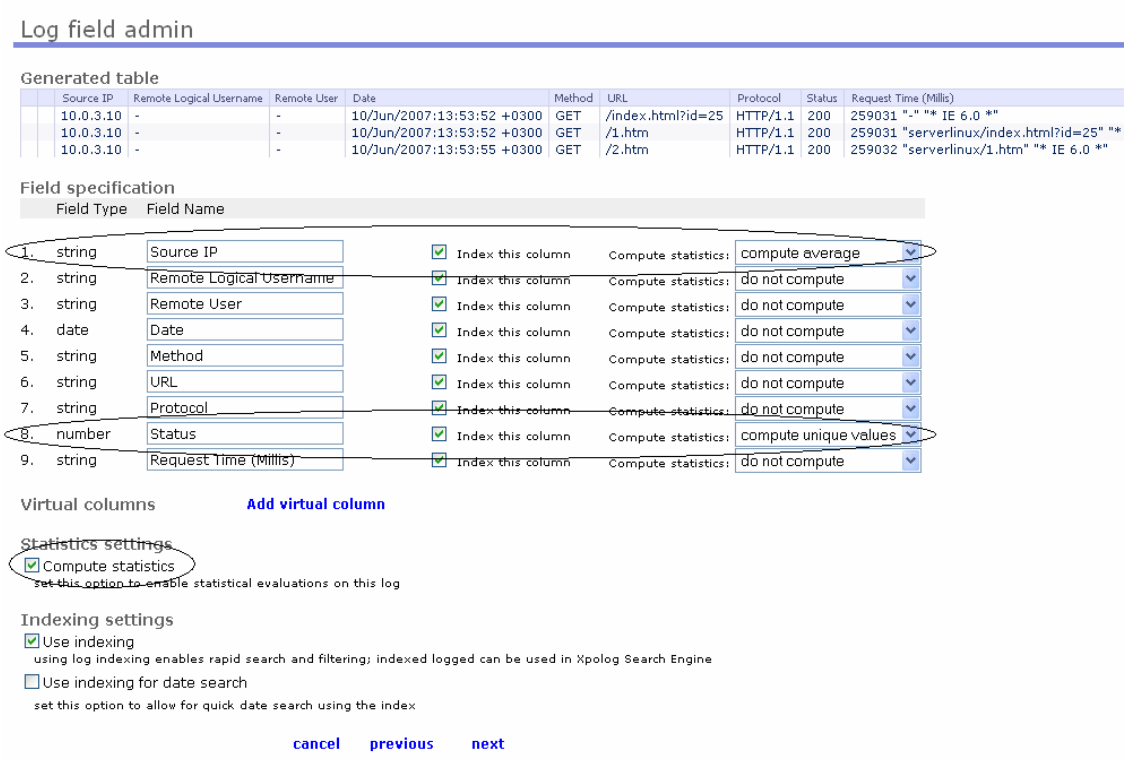


Figure 1 – Defining Log Statistics

Creating Dashboard Data:

There are 3 means for creating dashboard data:

- The first mean for creating dashboard data is by running the automatic configuration wizard. Once applications have been selected by the user and their configurations (their corresponding modules, logs and reports) created (steps 1 and 2 of the wizard), the wizard can continue to generate the dashboard data. Just press the 'Next' link to run both the reports of the created applications and the dashboard data generator. XpoLog will generate report data for each of the applications' reports for the last day, while the dashboard data generator will run on the applications' log data of the last month. To set a different time frame for the generation of the dashboard data, click, before pressing the 'Next' link, the 'Advanced' link and enter a different time rule - either in terms of from/to dates or in terms of previous/last days.

- The second mean for creating dashboard data is from the system health's control pane, as described above.
- The third mean for creating dashboard data is by setting the dashboard scheduler. To set the dashboard scheduler, do the following:
    1. After the dashboard component has been selected, select the 'Administration' menu.
    2. Click the 'Time Rule' tab to display the dashboard generation and display time rules.
    3. In the 'Health report execution' section set the time frame you want the dashboard data to be generated for. In the 'Run health and statistics on the pervious' entry set the time unit and the time amount (for instance 1 day - pervious day, or simply yesterday) to define that time frame.
- In the 'Scheduling' section, set the data do define when the dashboard data generation should occur. Select either the days of the weeks in which the execution should take place, or enter instead the days of the month and the desired months in which you want your job to run.

  After defining the days at which your job should be executed you define the time of the desired executions. You can enter either a specific time (in the 'Activate on the given hour' section) or define hours interval and minutes interval, so that on the selected days the operation will be executed in the given hours intervals and within each hour in the given minutes interval. For example, selecting in the

scheduling section 'Every month' and 'Every day' and then defining to iterate every three hours and within each hour every 20 minutes will cause the job to be executed every day at 00:20, 00:40, 01:00, 03:00, 03:20 and so on.

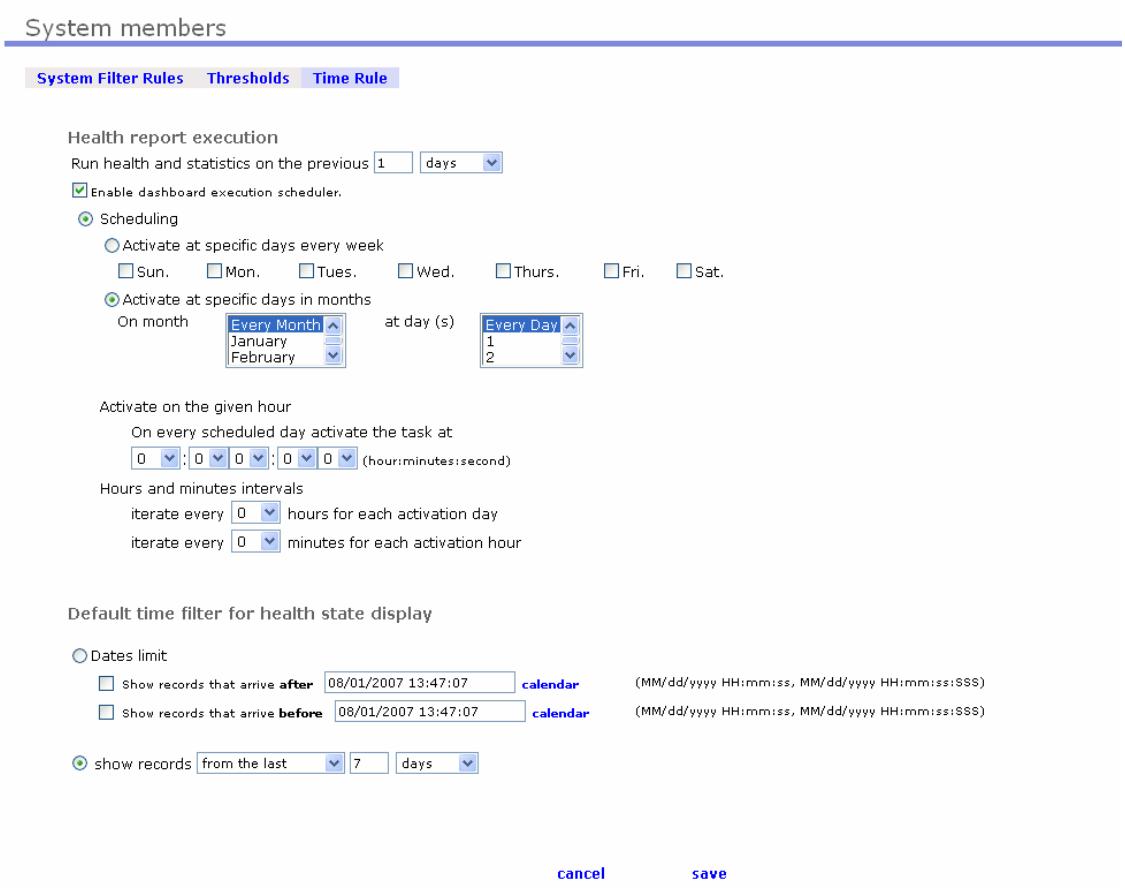


Figure … - Setting Dashboard Scheduler